Genetec™ Security Center.

Especificaciones de Security Center 5.10 A&E

CSI MasterFormat División 28

18 de diciembre de 2020

Genetec™

La información incluida en la presente es información confidencial y sujeta a derechos de propiedad intelectual de Genetec Inc.

Índice

Sección 28 13 00 – Software de Control de Acceso y Administración de Base de Datos 8

Parte 1 - Información General 8

1.01 Trabajo relacionado 8

1.02 Definiciones 8

1.03 Requisitos 8

Parte 2 - Productos 9

2.01 Requisitos generales del sistema electrónico de control de acceso 9

2.02 Requisitos de conmutación por error y espera 10

2.03 Administración de acceso del ACS 10

2.04 Administración Global de Tarjetahabientes ACS *(Especificador: se requiere licencia adicional y solo Enterprise para el sitio central*) 11

2.05 Lista de compatibilidad de hardware del ACS 12

2.06 Unificación continua con VMS 14

2.07 Administración (unidad) del controlador del ACS 14

2.08 Administración de Tarjetahabientes y Grupos de Tarjetahabientes del ACS 15

2.09 Administración de Credenciales del ACS 15

2.10 Formatos Personalizados de Tarjeta del ACS 16

2.11 Diseñador de Distintivos del ACS 17

2.12 Administración de puerta del ACS 18

2.13 Administración de elevador del ACS 19

2.14 Administración de Visitantes del ACS *(Especificador: se requiere licencia adicional)* 19

2.15 Conteo de Personas ACS y Seguimiento de Presencia en el Área (Agrupación) *(Especificador, se requiere licencia adicional)* 20

2.16 Campos personalizados de ACS (campos definidos por el usuario) 22

2.17 Import tool del ACS *(Especificador: se requiere licencia adicional)* 22

2.18 Requisitos Generales de Software de Clientes 23

2.19 Configuración de la interfaz de usuario (UI) 25

2.20 Interfaz de usuario (UI) de cliente ACS 26

2.21 Requisitos de la Interfaz de Usuario del Administrador del Servidor 30

2.22 Requisitos Generales del Unified Web Client (UWC) 31

2.23 Requisitos Generales para Aplicaciones para Teléfonos Inteligentes y Tabletas 32

2.24 Monitor de salud 35

2.25 Requisitos Generales de la USP 36
2.26 Arquitectura de la USP 38
2.27 Control de acceso USP, video y unificación ALPR 42
2.28 Administración de Alarmas de la USP 43
2.29 Niveles de amenaza de la USP *(Especificador: se requiere licencia adicional; solo Enterprise)* 44
2.30 Administración Avanzada de Tareas de la USP 45
2.31 Informes de la USP 45
2.32 Tableros de la USP 47
2.33 Característica de Federation de la USP: Monitoreo de sistemas remotos*(Especificador: solo Enterprise, licencia adicional obligatoria para cada sitio y entidad federada.)* 48
2.34 Administración de Zonas de la USP 48
2.35 Administración de Seguridad del Usuario y Grupo de Usuarios, Particiones y Privilegios de la USP 49
2.36 Administración de evento/acción de la USP 51
2.37 Programas y tareas programadas de la USP 51
2.38 Macros y Scripts Personalizados de la USP 52
2.39 Mapas gráficos dinámicos (DGM) de la USP 52
2.40 Auditoría y Registros de Actividades de Usuario de la USP (Registros) 57
2.41 Informes de Incidentes de la USP 58
2.42 Ingestión de datos de USP 58
2.43 Integración de terceros de USP 59
2.44 Kit de Desarrollo del Software (SDK, por sus siglas en inglés) de la USP *(Especificador: se requiere licencia adicional para Professional y versiones superiores)* 65
Parte 3 - Ejecución 66
3.01 Garantía 66
3.02 Puesta en marcha del sistema y servicios de integración *(Especificador, este es un cobro diario más viáticos, revisar Genetec Inc. para ver el número recomendado de días a especificar)* 66
3.03 Capacitación del Fabricante para el Operador Usuario Final *(Especificador: Este es un cargo de medio día más gastos)* 68
Sección 28 17 00 Sistema de Administración de Acceso e Identidad Física 70
Parte 1 - Información General 70
1.01 Trabajo relacionado 70
1.02 Definiciones 70
1.03 Requisitos 71

Parte 2 - Productos 71
Parte 1 - 71
Parte 2 - 71
2.01 Sistema de Administración de Acceso e Identidad Física (PIAM, por sus siglas en inglés) 71
Parte 1 - 72
Parte 2 - 72
2.02 Arquitectura 72
2.03 administración 74
Parte 3 - Ejecución 79
3.01 Ejecución 79
Sección 28 19 00 – Sistema de Identificación del Control de Acceso de Vehículos 83
Parte 1 - Información General 83
1.01 Trabajo relacionado 83
1.02 Definiciones 83
1.03 Requisitos 83
Parte 2 - Productos 84
2.01 Cámaras todo en uno SharpV 84
2.02 Aplicación del Software del Cliente 85
2.03 Interfaz de usuario de vigilancia (UI) 86
2.04 Requisitos de la Interfaz de Usuario del Administrador del Servidor 86
2.05 Requisitos Generales del Unified Web Client (UWC) 87
2.06 Monitor de salud 88
2.07 Requisitos Generales de la USP 89
2.08 Arquitectura de la USP 91
2.09 Unificación de USP ALPR, Video y Control de Acceso 95
2.10 Niveles de amenaza de la USP *(Especificador: se requiere licencia adicional; solo Enterprise)* 96
2.11 Tarea de la USP remota 97
2.12 Administración Avanzada de Tareas de la USP 98
2.13 Informes de la USP 98
2.14 Tableros de la USP 100
2.15 Característica de Federation de la USP: Monitoreo de sistemas remotos *(Especificador: solo Enterprise, licencia adicional obligatoria para cada sitio y entidad federada.)* 100

2.16 Administración de Seguridad del Usuario y Grupo de Usuarios, Particiones y Privilegios de la USP 101
2.17 Administración de evento/acción de la USP 102
2.18 Programas y tareas programadas de la USP 104
2.19 Macros y Scripts Personalizados de la USP 104
2.20 Mapas gráficos dinámicos (DGM) de la USP 105
2.21 Auditoría y Registros de Actividades de Usuario de la USP (Registros) 109
2.22 Informes de Incidentes de la USP 110
2.23 Ingestión de datos de USP 110
2.24 Integración de terceros de USP 111
2.25 Kit de desarrollo de software (SDK) de la USP 114
Parte 3 - Ejecución 115
3.01 Garantía 115
3.02 Puesta en marcha del sistema y servicios de integración *(Especificador, este es un cobro diario más viáticos, revisar Genetec Inc. para ver el número recomendado de días a especificar)* 116
3.03 Capacitación del Fabricante para el Operador Usuario Final *(Especificador: Este es un cargo de medio día más gastos)* 117
Sección 28 23 00 - Sistema de Administración de Video 119
Parte 1 - Información General 119
1.01 Trabajo relacionado 119
1.02 Definiciones 119
1.03 Requisitos 119
Parte 2 - Productos 120
2.01 Requisitos generales del VMS 120
2.02 Requisitos de seguridad cibernética 122
2.03 Requisitos de conmutación por error y espera 124
2.04 Archivado 125
2.05 Auxiliary Archiver *(Especificador: se requiere licencia adicional; solo Enterprise)* .130
2.06 Standby Archiver *(Especificador: solo Enterprise, requiere una licencia adicional por DVS que conmutará por error)* 130
2.07 Archivado de nube 131
2.08 Transmisión de video del VMS 132
2.09 Capacidades de transferencia de archivos de video del VMS 133
2.10 Video Analíticas de Seguridad 133
2.11 Monitor de integridad de la cámara 135

2.12 Protector de Privacidad 135
2.13 Contador de personas 137
2.14 Requisitos Generales de Software de Clientes 138
2.15 Configuración de la interfaz de usuario (UI) 140
2.16 Interfaz de usuario (UI) de cliente VMS 142
2.17 Requisitos de la Interfaz de Usuario del Administrador del Servidor 149
2.18 Requisitos Generales del Unified Web Client (UWC) 150
2.19 Requisitos Generales para Aplicaciones para Teléfonos Inteligentes y Tabletas 151
2.20 Monitor de salud 154
2.21 Administración de Comunicación (CM) de Session Initiation Protocol (SIP) *(Especificador, se requiere licencia adicional para todas las versiones)* 155
2.22 Requisitos Generales de la USP 161
2.23 Arquitectura de la USP 163
2.24 Control de acceso USP, video y unificación ALPR 167
2.25 Niveles de amenaza de la USP *(Especificador: se requiere licencia adicional; solo Enterprise)* 169
2.26 Tarea de la USP remota 169
2.27 Administración Avanzada de Tareas de la USP 170
2.28 Informes de la USP 170
2.29 Tableros de la USP 172
2.30 Característica de Federation de la USP: Monitoreo de sistemas remotos*(Especificador: solo Enterprise, licencia adicional obligatoria para cada sitio y entidad federada.)* 173
2.31 Administración de Zonas de la USP 173
2.32 Administración de Seguridad del Usuario y Grupo de Usuarios, Particiones y Privilegios de la USP 174
2.33 Administración de evento/acción de la USP 176
2.34 Programas y tareas programadas de la USP 178
2.35 Macros y Scripts Personalizados de la USP 178
2.36 Mapas gráficos dinámicos (DGM) de la USP 178
2.38 Auditoría y Registros de Actividades de Usuario de la USP (Registros) 184
2.39 Informes de Incidentes de la USP 184
2.40 Ingestión de datos de USP 184
2.41 Integración de terceros de USP 185
2.42 Kit de desarrollo de software (SDK) de la USP 191
Parte 3 - Ejecución 192

3.01 Garantía 192
3.02 Puesta en marcha del sistema y servicios de integración *(Especificador, este es un cobro diario más viáticos, revisar Genetec Inc. para ver el número recomendado de días a especificar)* 192
3.03 Capacitación del Fabricante para el Operador Usuario Final *(Especificador: Este es un cargo de medio día más gastos)* 194
Sección 28 51 00 – Administración y Presentación de Información 195
Parte 1 - Información General 195
1.01 Trabajo relacionado 195
1.02 Definiciones 195
1.03 Requisitos 195
Parte 2 - Productos 196
2.01 Requisitos generales 196
2.02 Interfaz de Usuario Gráfica del CDMS 198
2.03 Administración de Incidente del CDMS 199
2.04 Informe de incidentes del CDMS 203
2.05 Administración Dinámica de Documentos del CDMS 205
2.06 Motor de reglas del CDMS 205
2.07 Motor de Flujo de Trabajo de Automatización del CDMS 206
2.08 Procedimiento Operativo Estándar del CDMS 207
2.09 Sistema del Control de Acceso Electrónico *(Especificador, seleccionar una de las siguientes opciones)* 209
2.10 Sistema de Administración de Videos *(Especificador, seleccione una de las siguientes opciones)* 209
2.11 Requisitos de la Interfaz de Usuario del Administrador del Servidor 209
2.12 Requisitos Generales para Aplicaciones para Teléfonos Inteligentes y Tabletas 210
2.13 Monitor de salud 212
2.14 Requisitos Generales de la USP 213
2.15 Arquitectura de la USP 215
2.16 Control de acceso USP, video y unificación ALPR 219
2.17 Niveles de amenaza de la USP *(Especificador: se requiere licencia adicional; solo Enterprise)* 221
2.18 Tarea de la USP remota 222
2.19 Administración Avanzada de Tareas de la USP 222
2.20 Informes de la USP 223
2.21 Tableros de la USP 224

2.22 Característica de Federation de la USP: Monitoreo de sistemas remotos*(Especificador: solo Enterprise, licencia adicional obligatoria para cada sitio y entidad federada.)* 225
2.23 Administración de Zonas de la USP 226
2.24 Administración de Seguridad del Usuario y Grupo de Usuarios, Particiones y Privilegios de la USP 227
2.25 Administración de evento/acción de la USP 228
2.26 Programas y tareas programadas de la USP 229
2.27 Macros y Scripts Personalizados de la USP 230
2.28 Mapas gráficos dinámicos (DGM) de la USP 230
2.29 Auditoría y Registros de Actividades de Usuario de la USP (Registros) 235
2.30 Informes de Incidentes de la USP 235
2.31 Ingestión de datos de USP 236
2.32 Integración de terceros de USP 237
2.33 Kit de desarrollo de software (SDK) de la USP 242
Parte 3 - Ejecución 243
3.01 Garantía 243
3.02 Puesta en marcha del sistema y servicios de integración *(Especificador, este es un cobro diario más viáticos, revisar Genetec Inc. para ver el número recomendado de días a especificar)* 244
3.03 Capacitación del Fabricante para el Operador Usuario Final *(Especificador: Este es un cargo de medio día más gastos)* 245

Sección 28 13 00 – Software de Control de Acceso y Administración de Base de Datos

Parte 1 - Información General

1.01 Trabajo relacionado

A. División 08 - Hardware para Puertas

B. División 14 - Requisitos Generales para Elevadores

C. Sección 28 23 00 – Videovigilancia

1.02 Definiciones

A. ACS - Sistema de Control de Acceso

B. CSA - Aplicación de Software del Cliente

C. DGM - Mapas Gráficos Dinámicos

D. ALPR – Reconocimiento Automático de Placas de Matrícula

E. SDK - Kit de Desarrollo de Software

F. GLM – Administración del Ciclo de Vida de Genetec

G. SSM - Módulo de Software del Servidor

H. UI - Interfaz de Usuario

I. USP - Plataforma Unificada de Seguridad

J. USW - Cliente Web Unificado

K. VMS - Sistema de Administración de Videos

1.03 Requisitos

A. El programador del sistema deberá haber asistido a la capacitación del fabricante y obtenido la Certificación Técnica Security Center - Synergis™ de Genetec™.

B. Como opción, el programador del sistema deberá haber asistido a la capacitación del fabricante y obtenido la Certificación Técnica en Security Center - Enterprise de Genetec.

C. El programador del sistema deberá ser un Socio de Negocios Certificado Genetec con el siguiente nivel de preparación: *(Especificador: seleccione una de las siguientes opciones)*

Socio de Negocios Certificado o superior

Socio de Negocios Élite o superior

Socio de Negocios Élite Unificado

A. El programador del sistema deberá presentar comprobante de las certificaciones.

Parte 2 - Productos

2.01 Requisitos generales del sistema electrónico de control de acceso

A. El ACS deberá ser una solución de software de control de acceso por IP de clase empresarial. Deberá estar totalmente integrada dentro de una Plataforma de Seguridad Unificada (USP). La USP deberá permitir la unificación transparente del ACS con un sistema de administración de videos (VMS) IP.

B. El ACS deberá ser altamente escalable para soportar configuraciones que consisten de miles de puertas con instalaciones que abarcan múltiples zonas geográficas.

C. El ACS deberá soportar un número ilimitado de registros e historial de transacciones (eventos y alarmas) con el máximo permitido limitado por la cantidad de disco duro disponible.

D. El ACS deberá soportar una variedad de funcionalidades de control de acceso, los que incluyen pero no están limitados a:

1. Administración del Controller (Unidad), administración de puertas, administración de elevadores y administración de áreas.
2. Administración de tarjetahabientes y de grupos de tarjetahabientes, administración de credenciales y administración de las reglas de acceso.
3. Impresión de tarjetas de identificación y creación de plantillas.
4. Administración de Visitantes. *(Especificador, se requiere licencia adicional)*
5. Conteo de personas, rastreo de presencia en el área y agrupamiento.
6. Ofrecer una infraestructura para la integración de software de terceros, como un escáner para tarjetas y firmas.

E. Fabricante:

1. Genetec Security Center: *(Especificador: seleccione una de las siguientes opciones)*
   a. Synergis Enterprise
   b. Synergis Professional
   c. Estándar de sinergia

F. Certificación

1. El ACS deberá estar certificado en:
   a. UL-294

b. ULC-S319

c. EN-60839-11-1

d. CSPN

2.02 Requisitos de conmutación por error y espera

A. La USP deberá soportar opciones de conmutación por error nativas y las que se adquieren libremente en el mercado.

B. Directory de Conmutación por Error *(Especificador: se requiere licencia adicional por servidor que conmutará por error, solo Enterprise)*

1. El Directory en Modo de Espera deberá actuar como un SSM de reemplazo en estado de espera rápida, listo para actuar como el Directory actual en caso de falla del Directory principal. La conmutación por error deberá presentarse en menos de 1 minuto. No será necesaria ninguna acción por parte del usuario.

2. La USP deberá soportar hasta cinco (5) Directories en modo de espera, alineados para actuar como el Directory actual en una forma de cascada.

3. El Directory en Modo de Espera deberá conservar su base de datos de configuración sincronizada con el Directory principal.

4. El Directory en Modo de Espera deberá soportar escenarios de recuperación ante desastres en donde un servidor puede estar ubicado en otra área geográfica (o edificio) y encargase solamente si todos los otros directorios pasan a estar fuera de línea.

5. El Directory en Modo de Espera deberá soportar la sincronización de las bases de datos de configuración usando un mecanismo de copia de seguridad y restauración. El período de sincronización se podrá configurar desde 15 minutos hasta una semana.

6. El Directory en Modo de Espera deberá soportar la sincronización en tiempo real de las bases de datos de configuración que usan SQL Mirroring o SQL Always On.

C. Las opciones de modo de espera/conmutación por error adquiridas de forma libre en el mercado (sin incluir el Archiver del VMS) deberán incluir: *(Especificador: se requiere licencia adicional por servidor que conmutará por error; solo Enterprise)*

1. La conmutación por error de la función nativa en varios servidores

2. Clústeres de Windows

3. NEC ExpressCluster X LAN

2.03 Administración de acceso del ACS

A. El ACS deberá estar basado sobre una arquitectura abierta capaz de soportar múltiples fabricantes de hardware de control de acceso. El ACS deberá ser capaz de

integrarse con múltiples módulos y controladores de interfaz sin derechos de propiedad intelectual, lectores de acceso, y otras aplicaciones de terceros.

B. El ACS deberá ser una solución habilitada para IP. Toda la comunicación entre el ACS y los controladores de hardware deberá estar basada en el protocolo estándar TCP/IP.

C. Función del Access Manager

1. La función del Access Manager deberá ser el de servidor que sincroniza todas las unidades de hardware de control de acceso bajo su control, como lo son los controladores de puertas y los módulos E/S. Además debe ser capaz de validar y registrar todas las actividades y eventos de acceso cuando los controladores de puertas y los módulos E/S están en línea.

2. La función del Access Manager deberá mantener el enlace de comunicación con los controladores de hardware bajo su control. También deberá monitorear de forma continua si los controladores están en línea o fuera de línea.

3. La sincronización de las unidades de hardware deberá ser automatizada y transparente para los usuarios y deberá ocurrir en el trasfondo. También deberá ser posible sincronizar las unidades de forma manual o sincronizar las unidades dentro de un horario.

4. La Función del Access Manager deberá soportar puertas y controladores ubicados dentro de una o más instalaciones. El Servidor de Acceso deberá soportar un mínimo de 200 lectores y hasta 2000 lectores por computadora.

D. El Servidor de Acceso deberá almacenar todos los eventos de acceso asociados con las puertas, áreas y zonas de hardware (puntos de entrada de hardware), elevadores y controladores bajo su control directo.

2.04 Administración Global de Tarjetahabientes ACS *(Especificador: se requiere licencia adicional y solo Enterprise para el sitio central*)

A. El ACS deberá soportar la administración global de tarjetahabientes y la sincronización entre un sitio central independiente y sitios remotos independientes, todos los cuales tienen su propio Directory y bases de datos.

B. Deberá ser posible sincronizar las siguientes entidades y sus datos de configuración:

1. Tarjetahabientes (incluyendo campos personalizados)

2. Grupos de tarjetahabientes

3. Credenciales

4. Plantillas de tarjetas de identificación

C. Los tarjetahabientes y otras entidades sincronizadas se pueden agregar de forma central y sincronizarse a sitios remotos para la administración central de tarjetahabientes.

D. Los tarjetahabientes y otras entidades sincronizadas se pueden agregar a sitios remotos y sincronizarse con el sitio central y otros sitios remotos.

E. El ACS deberá soportar la asignación de una sola tarjeta por tarjetahabiente a lo largo de todos los sitios de la organización.

F. Deberán soportarse la sincronización manual y programada.

G. El ACS deberá soportar el comando OSDP del fabricante.

2.05 Lista de compatibilidad de hardware del ACS

A. El ACS deberá tener una arquitectura abierta que soporte la integración de controladores de puerta con base IP y módulos E/S de terceros. El ACS deberá soportar de forma simultánea configuraciones mixtas de hardware de control de acceso de múltiples proveedores.

B. El ACS deberá admitir el SAM integrado para retener claves de encriptación de DESfire.

C. El ACS deberá soportar la autenticación 802.1x.

D. El ACS deberá soportar el motor de validación de certificados integrados.

E. El ACS deberá soportar el uso de TLS 1.2 y certificados.

F. El ACS deberá admitir el Canal Seguro OSDP.

G. El ACS deberá admitir el modo de lector transparente OSDP para leer credenciales DESfire.

H. El ACS deberá soportar múltiples tipos de dispositivos de hardware: controladores con un solo lector, controladores con 2 lectores, controladores de 1 a 64 lectores, lectores integrados y controladores de puerta, y controladores de puerta habilitados para alimentación a través de Ethernet (PoE).

I. El ACS admitirá la mayoría de los lectores de tarjeta estándar de la industria que producen datos de tarjeta usando el protocolo OSDP y Wiegand, así como Clock-and-Data.

J. El ACS deberá soportar los siguientes controladores habilitados para IP. Para ver la descripción de las capacidades del controlador, consulte las especificaciones y diseño A&E del controlador específico:

1. Controlador Synergis Master
2. Synergis Cloud Link
3. Synergis
4. SharpV
5. HID VertX

6. HID VertX EVO
7. HID Edge
8. HID Edge EVO
9. Controladores PW6000
10. Controladores EP Mercury
11. Controladores LP Mercury
12. Módulo SIO Mercury
13. Puente Mercury M5
14. Puente Mercury MS
15. Concentrador de 8 a 1 Assa Abloy Aperio RS485
16. Concentrador AH40 (IP) Assa Aperio
17. Cerraduras Assa Abloy IP (no requieren DSR)
    a. Corbin Russwin
    b. Pasaporte Sargent
    c. Perfil Sargent
    d. IN220
18. Salto Sallis RS485 y enrutadores PoE
19. Salto SVN
20. Cerraduras electrónicas Schlage AD-300 y AD-400
21. Cerraduras inalámbricas Schlage Control
22. Cerraduras embutidas para red inalámbrica Schlage NDE, LE, FE y BE en red
23. Eje A1001
24. Eje A1601
25. Lectores STid RS485
26. DDS AS34 / TPL4
27. SimonsVoss Smart Intego

K. Se deberán soportar los siguientes lectores de registro de USB: *(Especificador: se requiere licencia adicional)*

1. Lector RF Ideas pcProx HID USB para registrar tarjetas de proximidad
2. Lector RF Ideas AIR ID Enroll iCLASS ID# USB para tarjetas de registro HID iCLASS

3. Lector RF Ideas AIR ID Enroll 14443/15693 CSN USB para registrar una tarjeta MIFARE usando el CSN (número de serie de la tarjeta)
4. Lector RF Idea AIR ID Enroll pcProx Plus con iCLASS para registrar tarjetas de proximidad y iCLASS
5. STid STR-W35-E / PH5-5AA
6. Lectores HID Omnikey 5x2x USB

2.06 Unificación continua con VMS

A. A través de la USP, el ACS podrá soportar la integración con un Sistema de Videovigilancia por IP o MVS. La integración con un sistema de videovigilancia por IP deberá permitir al usuario ver video en vivo y grabado.

B. Los usuarios podrán asociar una o más cámaras de video a los siguientes tipos de entidades: puertas, elevadores, zonas de hardware (puntos de entrada) y otras.

C. La UI de Monitoreo deberá presentar una verdadera Interfaz Unificada de Seguridad para el control de acceso y la videovigilancia. La visualización y reproducción avanzada de vídeo en vivo de vídeo archivado deberá estar disponible a través de la UI de Monitoreo.

D. Deberá ser posible ver los videos asociados con los eventos de control de acceso cuando se visualiza un informe.

2.07 Administración (unidad) del controlador del ACS

A. El ACS deberá soportar el descubrimiento, configuración y administración de los controladores habilitados para IP y los módulos E/S (unidades de hardware). Un usuario tendrá permitido agregar, borrar o modificar un controlador si cuenta con los privilegios correspondientes.

B. El ACS deberá soportar la configuración de unidades a través de una plantilla de puerta preconfigurada.

C. El ACS deberá soportar la detección automática de la unidad. El usuario deberá establecer las configuraciones para los puertos de descubrimiento y para los tipos de descubrimiento de unidad, y el ACS deberá automáticamente detectar todos los dispositivos conectados.

D. El ACS deberá soportar una herramienta de unidad de espacio de intercambio para intercambiar un controlador existente con un controlador nuevo. El servicio de intercambio de unidad deberá evitar la reprogramación del sistema cuando se reemplaza una unidad. Deberán mantenerse todos los registros y eventos de la unidad antigua.

E. El ACS deberá soportar la preconfiguración del sistema antes de la instalación física del hardware.

F. El ACS deberá soportar actualizaciones masivas de la aplicación

G. El ACS deberá admitir la administración central de la configuración de MIFARE DESfire.

2.08 Administración de Tarjetahabientes y Grupos de Tarjetahabientes del ACS

A. El ACS deberá soportar la configuración y la administración de los tarjetahabientes y grupos de tarjetahabiente. Un usuario podrá agregar, borrar o modificar un tarjetahabiente o grupo de tarjetahabientes si cuenta con los privilegios correspondientes.

B. Los campos personalizados deberán ser soportados, tanto los de tarjetahabientes como los de grupos de tarjetahabientes.

C. El ACS deberá permitir las siguientes opciones de activación/vencimiento para el perfil de un tarjetahabiente: activación retardada del perfil de un tarjetahabiente, vencimiento con base a la fecha del primer uso de las credenciales, o vencimiento en una fecha definida de un usuario.

D. Se podrá fijar una fecha de inicio y una fecha de vencimiento para la asociación de un tarjetahabiente y una regla de acceso para el acceso temporal.

E. Será posible asociar una foto con el perfil del tarjetahabiente. La foto deberá ser importada desde un archivo, capturada con una cámara digital, o capturada desde una cámara de videovigilancia. Cuando ocurra un evento de tarjetahabientes, la foto del tarjetahabiente deberá ser visualizada en la UI de Monitoreo. El ACS deberá soportar múltiples formatos de fotos estándar.

F. Los grupos de tarjetahabientes deberán habilitar el agrupamiento de tarjetahabientes para facilitar los cambios masivos a las configuraciones del sistema. Deberá ser posible asignar grupos de tarjetahabientes a reglas de acceso, evitando con esto la asignación de un tarjetahabiente a la vez.

G. Deberá ser posible buscar por asociación de fotos, campos personalizados, nombres y códigos de credenciales.

H. Deberá ser posible seleccionar varios tarjetahabientes para la desactivación o reactivación inmediata.

I. El ACS deberá soportar la sincronización de tarjetahabientes y el grupo de tarjetahabientes a través de un Active Directory que incluye credenciales y fotos de los tarjetahabientes. *(Especificador, la integración del Active Directory requiere una licencia y está disponible en Professional y versiones superiores.)* Deberá ser posible importar tarjetahabientes desde el Active Directory de Azure.

J. Deberá soportar la capacidad de rastrear credenciales sin usar durante x días

2.09 Administración de Credenciales del ACS

A. El ACS deberá soportar la configuración y administración de credenciales, como tarjetas de acceso y números PIN de teclados. Un usuario será capaz de agregar, eliminar o modificar una credencial si el usuario cuenta con los privilegios correspondientes.

B. El ACS deberá soportar el modo transparente de lector.

C. Los usuarios deberán ser capaces de agregar Campos Personalizados (campos definidos por el usuario) a las credenciales. La creación de una nueva credencial podrá hacerse de forma manual o automática.

D. La creación automática deberá permitir al usuario crear una entidad de credencial al presentar una credencial a un lector seleccionado. El ACS deberá leer los datos de la tarjeta y asociarlos con la entidad de la credencial. Deberá ser posible la inscripción automática de cualquier formato de tarjeta.

E. El ACS admitirá credenciales de alta seguridad mediante la validación de un certificado, como PIV, PIV-I y CIV.

F. El ACS deberá soportar credenciales múltiples por tarjetahabiente sin la necesidad de duplicar la información del tarjetahabiente. El ACS deberá detectar y evitar de forma automática los intentos para registrar una credencial ya registrada.

G. Deberá ser posible codificar de forma nativa las credenciales DESfire desde la interfaz de usuario utilizando las claves y la configuración del cliente.

H. Deberá soportar la inscripción de lotes de credenciales.

I. El ACS deberá proporcionar un flujo de trabajo para la emisión de tarjetas de identificación y solicitudes de tarjeta.

J. Deberá ser posible soportar credenciales PIV en el sistema de manera nativa.

K. El ACS deberá soportar el uso de las placas de matrícula como credenciales.

L. El ACS deberá soportar pines de coerción.

M. El ACS deberá soportar, de forma nativa, la creación y administración de identificaciones móviles de la misma manera que otras credenciales.

2.10 Formatos Personalizados de Tarjeta del ACS

A. Una característica del formato personalizado de tarjeta deberá permitir al administrador agregar formatos adicionales de tarjetas personalizadas usando una herramienta intuitiva dentro de la UI de Configuración. La herramienta de formato personalizado de tarjeta deberá contar con la siguiente flexibilidad:

1. Una vez inscrito, los nuevos formatos personalizados de tarjeta deberán aparecer en las listas de formato de tarjeta para la inscripción manual de la tarjeta.

2. Se pueden agregar un número ilimitado de formatos adicionales de tarjeta personalizada.

3. Deberá soportar credenciales con hasta 256 bits.

4. El administrador deberá ser capaz de establecer las siguientes opciones al definir un formato nuevo:

a. El orden en que aparecen los campos de la tarjeta en la interfaz de usuario o CSA.

b. Si un campo está escondido o es visible para un operador.

c. Si un campo es de solo lectura o si se puede modificar por un operador.

d. Esquemas complejos de revisión de paridad.

e. El orden y la ubicación de la información del campo. La ubicación se puede definir en base a bit en bit.

f. ID de la aplicación y claves para las credenciales DESfire EV1.

2.11 Diseñador de Distintivos del ACS

A. El diseñador de tarjetas de identificación deberá permitir la creación de plantillas para tarjetas de identificación que definan el formato del contenido y la presentación de la tarjeta de identificación del tarjetahabiente a imprimir.

B. La producción de la tarjeta de identificación deberá consistir en seleccionar la credencial y la plantilla de la tarjeta, y hacer clic en imprimir.

C. Deberá estar disponible la capacidad de imprimir lotes de tarjetas.

D. El contenido de una plantilla de las tarjetas de identificación puede incluir: nombre y apellido del tarjetahabiente, foto, campos personalizados, gráficos de mapas de bit, líneas, óvalos, rectángulos, etiquetas de texto dinámico enlazados a campos personalizados y etiquetas de texto estático, y códigos de barra (Intercalados 2 de 5, Código Extendido 39).

E. Deberá estar disponible la capacidad de copiar y pegar objetos de plantillas de tarjetas de identificación.

F. Deberá ser posible definir el grosor y el color del borde, el color de relleno de los objetos de la tarjeta de identificación (contenido) y el color de las etiquetas de texto.

G. Las configuraciones, como la transparencia del objeto, orientación de texto, y tamaño automático de texto deberán estar disponible o ser transparente para el usuario.

H. Los formatos de soporte de las tarjetas de identificación deberán ser (vertical y horizontal): CR70 (2,875 in x 2,125 in), CR80 (3,37 in x 2,125 in), CR90 (3,63 in x 2,37 in), CR100 (3,88 in x 2,63 in) y tamaños personalizados de tarjeta.

I. Se deberán soportar tarjetas de identificación de doble cara.

J. Deberá estar disponible una función de importación y exportación de plantillas de tarjetas de identificación para permitir compartir plantillas de tarjetas de identificación distintas o independientes del ACS.

K. Deberá soportar Chromakey.

2.12 Administración de puerta del ACS

A. El ACS deberá soportar la configuración y la administración de puertas. Un usuario podrá agregar, borrar o modificar una puerta si cuenta con los privilegios correspondientes.

B. El ACS deberá permitir que reglas de acceso múltiples se asocien a una puerta.

C. Deberá ser posible desbloquear todas las puertas de un área al mismo tiempo.

D. El ACS deberá soportar las siguientes formas de autenticación: Solo Tarjeta, Tarjeta o Teclado (PIN) o Tarjeta y Teclado (PIN). Deberá ser posible definir un horario para cuando se requieran modos de autenticación de Solo Tarjeta o Tarjeta y Teclado.

E. Deberá ser posible establecer un tiempo de autorización extendido con base a cada puerta (además del tiempo de autorización estándar). Las propiedades del tarjetahabiente deberán incluir la opción de usar el tiempo de autorización extendido. Cuando se otorga acceso a tarjetahabientes seleccionados, la puerta será desbloqueada durante el tiempo de autorización extendido en vez del tiempo de autorización estándar.

F. El ACS deberá permitir la configuración del modo de rebloqueo en las puertas, como por ejemplo, en puerta abierta, después de un tiempo definido, o en puerta cerrada.

G. El ACS deberá soportar la habilidad de hacer cumplir el uso de dos lecturas válidas de diferentes tarjetahabientes para otorgar el acceso a un área.

H. El ACS deberá soportar la capacidad para habilitar las reglas de acceso para otros tarjetahabientes una vez que un supervisor ha ingresado a un área.

I. El ACS deberá soportar la capacidad de habilitar un horario de desbloqueo en una puerta una vez que un empleado ha ingresado a la instalación.

J. Puertas sin lectores.

1. El ACS deberá soportar las puertas configuradas únicamente con una cerradura, un REX y un contacto de puerta pero sin lectores.

2. La implementación de una puerta sin lector deberá ser posible con el uso de módulos estándares de hardware de acceso E/S. No se requerirá hardware externo, como temporizadores.

3. Los horarios de desbloqueo deberán ser programables para las puertas sin lector.

4. Los informes estándar de actividad de puertas también deberán ser posibles con las puertas sin lector.

K. Los horarios de desbloqueo y las excepciones para los horarios de desbloqueo deberán estar asociados con una puerta. El horario de desbloqueo deberá determinar cuándo se debe desbloquear automáticamente una puerta. El ACS deberá soportar además el uso de un horario específico de desbloqueo fuera de línea. Las excepciones a los horarios de desbloqueo deberán usarse para definir

períodos de tiempo durante los cuales no se pueden aplicar los horarios de desbloqueo, como por ejemplo, durante los días feriados oficiales.

L. El ACS deberá soportar una o más cámaras por puerta. El video deberá asociarse con los eventos de acceso de puertas, tales como el acceso otorgado o negado.

2.13 Administración de elevador del ACS

A. El ACS deberá soportar la configuración y la administración de elevadores. Un usuario podrá agregar, borrar o modificar un elevador si cuenta con los privilegios correspondientes.

B. El ACS deberá ser capaz de controlar el acceso a pisos específicos usando un lector dentro de la cabina del elevador. El control deberá estar disponible a través del uso de un controlador con una interfaz a un lector y a múltiples módulos de salida con retransmisión.

C. Las selecciones de piso del elevador se rastrearán usando un controlador con una interfaz a múltiples módulos de entrada. El rastreo por pisos estará disponible dentro de un informe de actividades de elevador.

D. El módulo de control del elevador deberá seguir funcionando en el modo fuera de línea si hay una falla de comunicación entre el ACS y el controlador.

E. El ACS deberá soportar una o más cámaras por cabina de elevador. El video deberá asociarse a los eventos de acceso del elevador, como acceso otorgado o negado.

2.14 Administración de Visitantes del ACS *(Especificador: se requiere licencia adicional)*

A. El ACS deberá soportar la configuración y la administración de visitantes. Un usuario podrá registrar o borrar un visitante si cuenta con los privilegios correspondientes. El ACS deberá soportar el registro de las entradas y el registro de las salidas de visitantes desde la UI de Monitoreo.

B. Un asistente de registro de entradas de un visitante deberá facilitar el proceso del registro, permitiendo al usuario detallar la información específica del visitante.

C. Deberá ser posible definir un anfitrión que vaya delante del grupo de visitantes y una que vaya detrás para activar una alarma si un visitante no sigue la delegación.

D. El ACS deberá permitir las siguientes opciones para la credencial durante el registro de entrada del visitante:

1. Usar una credencial existente.
2. Crear automáticamente una nueva credencial.
3. Crear de manera manual una nueva credencial.

E. El ACS deberá soportar la creación de un grupo de credenciales de visitante por anticipado. Las credenciales existentes de visitantes deberán asignarse a visitantes durante el proceso de registro de entrada.

F. El ACS deberá permitir a los grupos de tarjetahabientes ser designados como «disponible para visitantes». Los usuarios podrán definir privilegios de acceso para los grupos de tarjetahabientes (grupos de tarjetahabientes para visitantes) por anticipado. Durante el registro de entrada del visitante, el usuario deberá seleccionar el grupo de tarjetahabientes para visitantes adecuado para asociarlo con el visitante. Todos los privilegios de acceso del grupo de tarjetahabientes para visitantes deberán transferirse de forma automática al visitante. Esta característica deberá permitir la creación de múltiples tipos de grupos visitantes y privilegios correspondientes, como para contratistas, VIPs y visitantes diarios. Los visitantes agregados a un grupo de tarjetahabientes para visitantes en la UI de Monitoreo deberán actualizarse automáticamente en la pantalla de la UI de Configuración del grupo de tarjetahabientes.

G. El perfil del visitante deberá soportar la modificación en tiempo real de la información del visitante después del registro de entrada del visitante.

H. El ACS deberá proporcionar además un rastreo integral de visitantes y generación de informes de visitantes. A través de la característica de seguimiento en tiempo real, el ACS deberá generar un listado histórico de actividades de visitante y de tiempo real en la UI de Monitoreo. El ACS deberá generar además informes específicos de visitantes que ofrecen un listado completo de visitantes al igual que detalles completos sobre su movimiento.

I. Deberá ser posible exonerar a un visitante de cualquier regla antirretorno válida.

J. El operador deberá ser capaz de imprimir tarjetas de identificación de visitantes durante el proceso de registro de entrada. Deberá soportar la impresión tanto de tarjetas de identificación en papel (visitante sin una credencial asignada) como credenciales reales.

K. La administración y la generación de informes de visitantes deberán estar disponible también a través del Web Client.

L. Deberá ser posible encontrar la información o el perfil de un visitante al deslizar la credencial del visitante (tarjeta) en un lector USB.

M. Se podrá etiquetar a la persona visitada con el perfil del visitante.

N. Se podrá requerir que el visitante cuente con un acompañante para ingresar a un área y que el acompañante deba registrar su tarjeta de identificación para confirmar el acceso del visitante.

O. El sistema del ACS deberá soportar soluciones de administración de visitantes de terceros. *(Especificador, se requiere licencia adicional)*

2.15 Conteo de Personas ACS y Seguimiento de Presencia en el Área (Agrupación) *(Especificador, se requiere licencia adicional)*

A. El ACS deberá soportar el conteo de personas (o el rastreo de presencia en el área). El ACS podrá monitorear e informar el número de tarjetahabientes en un área en tiempo real y en todas las áreas. El monitoreo se debe basar en toda la

infraestructura de control de acceso, tanto para las áreas locales como para aquellos sitios geográficamente remotos. El conteo de personas también se puede usar para realizar aglomeraciones.

B. Deberá ser posible controlar la máxima ocupación de un área si se define un umbral y una notificación para el usuario cuando se alcance el límite.

C. El ACS deberá reportar los conteos de presencia en el área en la UI. El rastreo de la presencia en el área rastreará de forma dinámica el número total de tarjetahabientes en un área. Los datos visualizados serán actualizados de forma dinámica.

D. El ACS deberá soportar el agrupamiento mediante el uso de lectores móviles (se requiere software y hardware adicional de terceros).

E. El ACS deberá proporcionar una tarea de agrupamiento dedicada y nativa a través de lectores USB, móviles y de pared.

F. El ACS deberá ser capaz de generar un informe de presencia en el área enumerando los tarjetahabientes ubicados en una o más áreas, accesible a través de la UI de Monitoreo. Será posible filtrar el informe por área y por período de tiempo. El informe incluirá además la actividad de subáreas (áreas anidadas).

G. A través del conteo de personas, el ACS podrá generar eventos de Primera Persona que Entra y Última Persona que Sale. El evento Primera Persona que Entra detectará cuando entra el primer tarjetahabiente a un área vacía. El evento Última Persona que Sale detectará cuando sale el último tarjetahabiente de un área. Se podrán activar acciones de ambos eventos, como enviar un mensaje o activar una alarma.

H. El ACS podrá determinar la entrada de un tarjetahabiente con base en un sensor dedicado.

I. El ACS deberá proporcionar un tablero de control HTML visual para ayudar con la evacuación que pueda ejecutarse en dispositivos móviles.

J. El ACS proporcionará la capacidad de ver globalmente todas las evacuaciones simultáneamente o por área.

K. En una evacuación, el ACS establecerá a todos los tarjetahabientes como desconocidos hasta que lleguen a un punto de reunión.

L. Será posible marcar a un tarjetahabiente como seguro o no seguro desde el asistente de evacuación web.

M. Será posible filtrar por grupos de tarjetahabientes o campos personalizados en el tablero de control.

N. El ACS admitirá lectores montados en la pared y dispositivos móviles para la reunión.

O. El ACS proporcionará una indicación visual clara cuando se esté evacuando un área.

P. El ACS tendrá la capacidad de configurar un punto de reunión por área.

Q. El ACS tendrá la capacidad de restablecer APB al final de una evacuación.

2.16 Campos personalizados de ACS (campos definidos por el usuario)

A. El ACS permitirá la creación de campos personalizados. Deberá soportar hasta 1,000 campos personalizados.

B. Los campos personalizados deberán estar soportados por las siguientes entidades: tarjetahabientes, grupos de tarjetahabientes, credenciales y visitantes.

C. Los campos personalizados admitidos deben incluir texto, números enteros, números decimales, fechas, valores booleanos e imágenes (gráficos).

D. Los usuarios podrán definir un valor predeterminado para un campo personalizado.

E. Se podrán crear nuevos tipos de campos personalizados. Los nuevos tipos de campos personalizados estarán basados en los campos estándar personalizados soportados. Deberán soportar valores definidos por el usuario de los cuales el operador tendrá que hacer una selección.

F. Los administradores tienen la habilidad de definir cuáles usuarios pueden ver y modificar campos personalizados específicos. Esto limitará el acceso a los datos de campos personalizados para usuarios con privilegios predefinidos. El ACS soportará la generación de consultas e informes usando campos personalizados.

G. Los campos personalizados pueden agruparse y ordenarse dentro de estos grupos en base a la definición del usuario.

H. Los valores para los campos personalizados se pueden importar usando la Import Tool.

2.17 Import tool del ACS *(Especificador: se requiere licencia adicional)*

A. El ACS soportará un Import Tool integrado para facilitar la importación de información existente de tarjetahabientes y credenciales. La importación de datos se llevará a cabo a través del uso de un formato de archivo CSV. La herramienta estará disponible desde la UI de Configuración.

B. Deberá ser posible conectarse a una base de datos de Microsoft SQL u Oracle externa para importar tarjetahabientes.

C. El Import Tool soportará además la habilidad para la importación manual de información que se ha exportado desde bases de datos de terceros si se están en el formato CSV.

D. El Import Tool permitirá la importación de los siguientes datos:

1. Nombre, descripciones, foto, correo electrónico y situación o categoría del tarjetahabiente.

2. Información del grupo de tarjetahabientes.
3. Nombre de credencial, situación o categoría, formato y número de tarjeta (incluyendo credenciales con formatos personalizados).
4. Información de partición.
5. Campos personalizados.
6. Fecha de activación y fecha de vencimiento.
7. Actualización a la asociación de grupo de tarjetahabientes.

E. Deberá contar con total flexibilidad para seleccionar los campos a importar durante una sesión de importación.

F. Deberá especificarse la opción de usar una clave única y personalizada del tarjetahabiente durante el proceso de importación para asegurar que no se sobrescriba sobre los datos de tarjetahabientes con nombres iguales. La generación de claves de tarjetahabiente deberá ser automatizada. El usuario final contará con la opción de seleccionar cuáles campos se usarán para crear esta clave única, como número de credencial, campos personalizados o nombre del tarjetahabiente.

G. El ACS también soportará la reimportación de archivos CSV que contengan nueva información para actualizar la información existente en la base de datos del ACS. La reimportación deberá habilitar las enmiendas en masa a la información de control de acceso existentes.

2.18 Requisitos Generales de Software de Clientes

A. Las Aplicaciones de Software de Cliente (CSA, por sus siglas en inglés) deberán proporcionar la interfaz de usuario para la configuración USP y el monitoreo sobre cualquier red, y estar accesibles de manera local o desde una conexión remota.

B. Las CSA deberán de consistir de la UI de Configuración para la configuración del sistema y el monitoreo de la UI de Monitoreo. Las CSA deberán tener una base Windows y proporcionar una interfaz de usuario (UI) gráfica fácil de usar.

C. Las CSA para monitoreo deberán soportar el funcionamiento en modo de 64 bits.

D. Se deberá usar el Server Administrator para configurar la(s) base(s) de datos del servidor. Deberá estar basado en la Web y ser accesible de forma local en el SSM o a lo largo de la red.

E. Las CSA deberán fusionarse de manera transparente con el control de acceso, el reconocimiento de placas de matrícula (ALPR, por sus siglas en inglés), y las funcionalidades de video dentro de la misma aplicación de usuario.

F. La USP deberá usar el desarrollo y las tecnologías de programación más recientes de interfaz de usuario (UI) como lo son Microsoft WPF (Windows Presentation Foundation), el lenguaje de marcado XAML, y la plataforma del software .NET.

G. Todas las aplicaciones deberán proporcionar un mecanismo de autenticación, el cual verifica la validez del usuario. Como tal, el administrador (quien cuenta con todos los derechos y privilegios) puede definir derechos y privilegios de acceso específicos para cada usuario en el sistema.

H. Se iniciará sesión en una CSA a través de cuentas y contraseñas de la USP almacenadas de manera local o a través de las credenciales del operador de Windows cuando esté habilitada la integración del Active Directory. *(Especificador: Professional y versiones superiores; se requiere licencia para Active Directory)*

I. Cuando está integrado con el Active Directory de Microsoft, la CSA y la USP deberán autenticar a los usuarios usando las credenciales de Windows. Como resultado de esto, la USP se beneficiará de la autenticación de contraseña y las poderosas características de seguridad del Active Directory. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

J. Cuando se integra con un proveedor de identidad externo como Windows Active Directory, ADFS (Active Directory Federation Services) o un proveedor de identidad de Open ID Connect/SAML2 (p. ej., Azure AD), la CSA y la USP deberán autenticar a los usuarios mediante una experiencia de Inicio de Sesión Única. Como resultado, la USP se beneficiará de volver a usar la misma credencial en todas las aplicaciones empresariales. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

K. La CSA deberá soportar múltiples idiomas, lo que incluye, entre otros, los siguientes: inglés, francés, árabe, checo, holandés, alemán, hebreo, húngaro, italiano, japonés, coreano, noruego, persa (farsi), polaco, portugués (Brasil), chino simplificado y tradicional, ruso, español, sueco, tailandés, turco y vietnamita.

L. Para mejorar la usabilidad y la eficiencia del operador, la UI de Configuración y la UI de Monitoreo deberán soportar muchas de las más recientes UI, como:

1. Una Página de Inicio personalizable que incluya tareas favoritas y usadas recientemente.
2. Un enfoque orientado a tareas para las actividades del administrador/operador en donde cada tipo de actividad (vigilancia, administración de visitantes, informes individuales, y otros) es una tarea del operador.
3. Flujos de trabajo consolidados y consistentes para videos, ALPR y control de acceso.
4. Funcionalidad con un solo clic para generación de informes y rastreo. La UI de Monitoreo deberá soportar tanto la generación de informes para el control de acceso, ALPR y videos con un solo clic, así como el rastreo de áreas, cámaras, puertas, zonas, tarjetahabientes, elevadores, entidades ALPR, y otras con un solo clic. La generación de informes o rastreos con un solo clic deberá crear una nueva tarea con las entidades seleccionadas a reportar o rastrear.

M. Página de Inicio y Tareas de la UI de Configuración y la UI de Monitoreo.

1. La UI de Configuración y la UI de Monitoreo deberán estar orientadas a tareas.

2. Una tarea deberá ser patrones de diseño de interfaz de usuario cuyo objetivo sea simplificar la interfaz de usuario al agrupar características similares desde diferentes sistemas como lo son video y acceso, en la misma ventana de visualización. Las características deberán agruparse juntas en una tarea con base en su habilidad compartida para ayudar al usuario a realizar una tarea específica.
3. Se tendrá acceso a las tareas a través de la Página de Inicio de la UI de Configuración o de las CSA de videovigilancia.
4. Las tareas recién creadas estarán accesibles a través de la barra de tareas de la UI de Configuración o de la UI de Monitoreo.
5. Las tareas similares deberán agruparse en las siguientes categorías:
   a. Funcionamiento: Administración de control de acceso, administración de LRP y otros.
   b. Investigación: informes de actividad de control de acceso, informes de actividad de visitantes, informes de alarmas, etc.
   c. Mantenimiento: Control de acceso y solución de problemas, registros de auditoría, informes relacionados con el estado de salud del sistema, etc.
6. Un operador solo será capaz de ejecutar una tarea específica si cuenta con los privilegios correspondientes.
7. El contenido de la Página de Inicio será personalizable a través del uso de privilegios para esconder tareas a las cuales no debería tener acceso un operador y a través de una lista de tareas favoritas y usadas recientemente. Además, será posible editar un archivo USP XML para agregar nuevas tareas sobre la marcha.

N. El contratista deberá proporcionar hasta XX número de clientes simultáneos. *(Especificador: las conexiones de cliente son simultáneas; se incluyen las primeras 5 conexiones de cliente; especifique la Licencia del Sitio después de 40 conexiones del cliente (solo Enterprise)*

2.19 Configuración de la interfaz de usuario (UI)

A. Información General

1. La aplicación de la UI de Configuración deberá permitir al administrador o a los usuarios con los privilegios adecuados cambiar la configuración del sistema. La UI de Configuración deberá proporcionar una configuración y administración descentralizada del sistema de la USP desde cualquier parte de la red IP.
2. La configuración de todos los sistemas ACS, VMS y ALPR embebidos será accesible a través de la UI de Configuración.
3. La UI de Configuración deberá tener una página de inicio con acceso a varias tareas con un solo clic.

4. La UI de Configuración deberá incluir una variedad de herramientas como herramientas para la solución de problemas, herramientas de importación, y una herramienta de detección de unidad, entre otras.
5. La UI de Configuración deberá incluir una interfaz de generación de informes estática para:
    a. Ver eventos históricos basado en la actividad de la entidad. El usuario será capaz de desempeñar acciones como imprimir un informe y solucionar un problema de un evento de acceso específico desde la vista de la generación de informes.
    b. Visualizar registros de auditoría que muestran un historial de los cambios que un usuario/administrador han hecho a una entidad.
6. Todos los sistemas incrustados (ACS, VMS y ALPR) podrán volver a usar las entidades comunes, como usuarios, horarios, alarmas y muchas más.

2.20 Interfaz de usuario (UI) de cliente ACS

A. La UI de Monitoreo deberá satisfacer la función de una Interfaz Unificada de Seguridad capaz de monitorear eventos de video, ALPR y control de acceso, al igual que visualizar video en vivo y grabado.

B. La UI de Monitoreo deberá proporcionar una interfaz de usuario gráfica para controlar y monitorear la USP sobre cualquier red IP. Deberá permitir a los administradores y operadores con los privilegios adecuados monitorear su plataforma unificada de seguridad, ejecutar informes y administrar alarmas.

C. Para mejorar la usabilidad y la eficiencia del operador, la UI de Monitoreo deberá soportar los siguientes conceptos de UI:
    1. Interfaz adaptable de forma dinámica que se ajusta en tiempo real a lo que está haciendo el operador.
    2. Controles dinámicos equipados con widgets específicos de las entidades (como widgets para puertas y cámaras).
    3. Uso de superposiciones transparentes que puedan mostrar múltiples tipos de datos de manera transparente.
    4. Visualización de menús de recuadros y comandos rápidos.
    5. Flujos de trabajo consolidados y consistentes.
    6. Menús de recuadros y comandos rápidos de fácil acceso dentro de cada recuadro visualizado del área de trabajo del usuario.
    7. Funcionalidad con un solo clic para generación de informes y rastreo. La UI de Monitoreo deberá soportar tanto la generación de informes para el control de acceso, ALPR y videos con un solo clic, así como el rastreo de áreas, cámaras, puertas, zonas, tarjetahabientes, elevadores, entidades ALPR, y otras con un solo clic. La generación de informes y rastreo con un solo clic deberá crear una nueva tarea con las entidades seleccionadas a reportar o rastrear.

D. Página de Inicio y Tareas de la UI de Monitoreo

1. Las tareas similares deberán agruparse en las siguientes categorías:

a. Funcionamiento: Control de acceso/LRP/videovigilancia, administración de visitantes, aglomeraciones, monitoreo de control de acceso y alarmas de videos, y otros.

b. Investigación: Informes de marcadores de video/movimientos/archivo, informes de actividades de control de acceso, informes de actividades de visitantes, informes de alarmas, informes de actividades ALPR, y otros.

c. Mantenimiento: Informes de control de acceso y configuración de videos, solución de problemas, registros de auditoría y mucho más.

E. UI Adaptable de Forma Dinámica, sección de Controles y Widgets

1. La UI de Monitoreo deberá adaptarse de forma dinámica a lo que está haciendo el operador. Esto se puede lograr a través de la agrupación de widgets en la sección de Controles de la UI de Monitoreo.

2. Los widgets deberán ser miniaplicaciones o miniagrupaciones en la sección de Controles de la UI de Monitoreo que permitan al operador desempeñar tareas comunes y proporcionarles un rápido acceso a información y acciones.

3. Con un solo clic sobre una entidad (como una puerta o cámara), aparece el widget específico asociado a dicha entidad y el resto de los widgets no relevantes desaparecen de forma dinámica (al instante). Los widgets le ofrecerán al operador información como el estado de la puerta e información de los flujos de las cámaras, al igual que acciones del usuario, como desbloqueo de puertas, controles PTZ, y otros.

4. Los widgets específicos incluyen aquellos para una puerta, cámara, alarma, zona, recuadro de visualización, transmisión de video (estadísticas), cámara PTZ, y otros.

F. Flujos de Trabajo del Operador

1. Un flujo de trabajo será una secuencia de operaciones que deberá ejecutar un operador o administrador para completar una actividad. El “flujo” se relaciona a una escala de tiempo o secuencia definida claramente para ejecutar la actividad.

2. La UI de Monitoreo deberá estar equipada con flujos de trabajo consistentes para ALPR, videos, y sistemas de control de acceso a los cuales unifica.

3. Generar o imprimir un informe, configurar o reconocer una alarma, o crear un informe de incidente deberá seguir el mismo proceso (flujo de trabajo) sin importar si el operador está trabajando con video, ALPR o control de acceso, o bien con ambos, video y control de acceso.

G. Cada tarea dentro de la UI de Monitoreo deberá consistir de uno o más de los siguientes elementos:

1. Lista de eventos.

2. Árbol lógico. Las puertas, cámaras, zonas, unidades ALPR y elevadores deberán estar agrupados bajo Áreas de una forma jerárquica.
3. Lista de entidades de todas las entidades que están siendo rastreadas.
4. Visualizar recuadros con varios patrones (1 x 1, 2 x 2, y otros).
5. Visualizar los menús de recuadros con varios comandos relacionados con cámaras, puertas, PTZ y controles de recuadros.
6. Sección de control con widgets.

H. La UI de Monitoreo deberá soportar múltiples listas de eventos y patrones de recuadros de visualización, entre los que se incluyen:

1. Solo el diagrama de las listas de eventos/alarmas
2. Solo el diagrama de los recuadros de visualización
3. Combinación de las listas de alarmas/eventos y recuadros de visualización
4. Combinación de las listas de alarmas/eventos y mapas ALPR

I. Personalización del área de trabajo del usuario

1. El usuario tendrá el control completo sobre el área de trabajo del usuario a través de una variedad de opciones de personalización seleccionadas por el usuario. Los administradores también serán capaces de limitar lo que los usuarios y operadores pueden modificar en su área de trabajo a través de privilegios.
2. Después de personalizar su área de trabajo, el usuario podrá guardarla.
3. El área de trabajo del usuario será accesible por un usuario específico desde cualquier aplicación de cliente en la red.
4. Los patrones de recuadros de visualización se podrán personalizar.
5. Las listas de eventos y alarmas se podrán colocar en cualquier parte de la pantalla, desde sólo una parte de la pantalla hasta la pantalla completa, y el usuario podrá cambiar su tamaño. La longitud de las listas de eventos o alarmas deberán ser definidas por el usuario. Las barras de desplazamiento deberán permitir al usuario navegar a través de largas listas de eventos y alarmas.
6. La UI de Monitoreo deberá soportar múltiples patrones de recuadros de visualización (como 1 recuadro de visualización (matriz 1x1), 16 recuadros (matriz 8x8), y múltiples variaciones adicionales).
7. La UI de Monitoreo deberá soportar tantos monitores como adaptadores de video de PC y el Sistemas Operativo Windows que sea capaz de aceptar.
8. Las opciones de personalización adicionales incluyen mostrar/ocultar paneles de ventana, mostrar/ocultar menús/barras de herramientas, mostrar/ocultar información superpuesta en videos, cambiar el tamaño de diferentes paneles de ventana y elegir el patrón de visualización de mosaicos por tarea.

J. La UI de Monitoreo deberá proporcionar una interfaz para soportar las siguientes tareas y actividades comunes al control de acceso, ALPR y videos:

1. Monitorear eventos desde un sistema de seguridad en vivo (ACS y/o VMS y/o ALPR).
2. Generar informes, incluyendo informes personalizados.
3. Monitorear y reconocer alarmas.
4. Crear y editar incidentes y generar informes de incidentes.
5. Visualizar planos y mapas gráficos y dinámicos, además de ejecutar acciones desde planos y mapas gráficos y dinámicos.
6. Administrar y ejecutar acciones y macros actuales.

K. La UI de Monitoreo será capaz de monitorear la actividad de las siguientes entidades en tiempo real: áreas, entidades ALPR, puertas, elevadores, cámaras, tarjetahabientes, grupos de tarjetahabientes, zonas (puntos de entrada), y otros. La UI de Monitoreo ofrecerá una interfaz para soportar las siguientes tareas y capacidades de control de acceso:

1. Monitoreo y administración de eventos y alarmas de acceso.
2. Visualización de la foto o tarjeta de identificación del tarjetahabiente.
3. Verificación de la foto que identifica al tarjetahabiente contra el video en vivo.
4. Administración de visitantes.
5. Conteo o aglomeraciones de personas, incluyendo la reconfiguración del conteo de personas en un área.
6. Control de puertas, incluyendo el desbloqueo remoto de puertas, la invalidación de los horarios de desbloqueo de una puerta, y la habilitación del modo de mantenimiento de la puerta.
7. Suspender el anti-retorno.
8. Generación de configuración del ACS e informes de actividades.
9. Visualización de archivos HTML incluyendo instrucciones para alarmas.

L. Monitoreo de la Entidad

1. La USP deberá permitir al usuario seleccionar múltiples entidades a monitorear desde la UI de Monitoreo al agregar las entidades una por una a la lista de seguimiento.
2. La UI de Monitoreo deberá ofrecer la opción de filtrar cuáles eventos deberán visualizarse en el plano de mosaicos de visualización, en el plano de la lista de eventos o en ambos.

3. Deberá ser posible bloquear un mosaico de visualización de la UI de Monitoreo de manera que solo rastree la actividad de una entidad específica (por ejemplo, una determinada puerta o cámara).

4. El usuario deberá ser capaz de arrastrar y soltar un evento desde una lista de eventos (o una alarma de una lista de alarmas) en un recuadro de visualización para ver una lectura de placa de matrícula , la foto que identifica al tarjetahabiente, la tarjeta de identificación, o video en vivo/archivado, entre otras opciones.

5. Las listas de eventos, alarma, monitoreo/rastreo y listas de informes deberán contener las fotos del tarjetahabiente cuando corresponda.

6. El usuario tendrá permitido iniciar o poner en pausa la visualización de eventos dentro de cada recuadro de visualización.

M. Empaquetar y Desempaquetar el Recuadro de Visualización

1. La UI de Monitoreo deberá soportar el empaquetado y desempaquetado con un solo clic para áreas, puertas, zonas y alarmas.

2. El empaquetado y desempaquetado de entidades permitirá a los operadores obtener rápidamente información adicional y vistas de cámara de una entidad específica.

3. El desempaquetado de una entidad deberá mostrar las entidades relacionadas. Por ejemplo, el desempaquetado de una puerta con múltiples cámaras asociadas deberá mostrar todas las cámaras asociadas con dicha puerta. El desempaquetado deberá volver a configurar los recuadros de visualización para que puedan mostrar todas las entidades asociadas. Por ejemplo, el desempaquetado de una puerta (o una zona o alarma) que tiene actualmente una configuración de recuadro 1 x 1 y que tiene 3 cámaras enlazadas a la misma creará un diagrama de recuadro de visualización de 1 x 3 para la visualización de todas las entidades asociadas.

4. El empaquetado devolverá la visualización al patrón original del recuadro.

N. Las siguientes herramientas o utilidades adicionales estarán disponibles desde la UI de Monitoreo: creación de credenciales, creación de tarjetahabientes y solucionador de problemas del control de acceso.

2.21 Requisitos de la Interfaz de Usuario del Administrador del Servidor

A. El Administrador del Servidor se usará para configurar el SSM y la Función de Directory (configuración principal) y su(s) base(s) de datos para aplicar la licencia, y otros más.

B. El Administrador del Servidor será una aplicación basada en la Web. A través del Administrador del Servidor será posible tener acceso al SSM a lo largo de la red o de forma local en el servidor.

C. El acceso al Administrador del Servidor estará protegido a través de un nombre de inicio de sesión, contraseña y comunicaciones encriptadas.

D. El Administrador del Servidor deberá permitir al administrador (usuario) realizar las siguientes funciones:

1. Administrar la licencia del sistema.
2. Configurar las bases de datos y el servidor de la base de datos para la Función de Directory.
3. Activar/ Desactivar la Función de Directory
4. Respaldar manualmente la(s) base(s) de datos de la Función de Directory y/o restaurar la(s) base(s) de datos del servidor, al igual que configurar las copias de seguridad programadas de las bases de datos.
5. Definir las configuraciones de seguridad de las comunicaciones entre el cliente y el servidor.
6. Configurar el hardware de comunicaciones de la red, incluidos las direcciones y los puertos de conexión.

2.22 Requisitos Generales del Unified Web Client (UWC)

A. La USP deberá soportar un cliente web unificado (UWC, por sus siglas en inglés) para el control de acceso, los videos y el reconocimiento automático de placas de matrícula (ALPR).

B. La UWC deberá ser un cliente verdaderamente ligero que no requiera de ninguna descarga con excepción de un navegador de web o plugins estándar de navegador de web.

C. La UWC será independiente de plataformas y se ejecutará dentro de Microsoft Edge, MS Internet Explorer, Firefox, Safari y Google Chrome.

D. El UWC deberá diseñarse como una aplicación HTML5.

E. El UWC deberá soportar la visualización en formato de tableta.

F. El UWC soportará videos nativos H.264 en el Cliente Web.

G. Las páginas web para el Web Client serán administradas e insertadas por el servidor Web Client. No será necesario Microsoft IIS ni ningún otro servicio de hospedaje de sitios web debido a que todas las páginas web serán hospedadas por el Mobile Server.

H. El Web Client Server deberá proporcionar la capacidad de definir una URL única para acceder al Web Client, a fin de garantizar la seguridad de la aplicación.

I. El UWC proporcionará la capacidad de cargar un plano de cámara.

J. El UWC proporcionará la habilidad de configurar, guardar y volver a cargar los diagramas privados de la cámara.

K. El UWC proporcionará la habilidad de controlar las Cámaras PTZ.

L. Funcionalidades:

1. El soporte para iniciar sesión estará disponible mediante:
    a. Nombre de usuario y contraseña
    b. Active Directory *(Specifier, Professional y superior, se requiere licencia adicional para Active Directory)*
    c. Proveedor de identidad Azure Active Directory, ADFS, OpenID Connect o SAML2 *(Especificador, Profesional y superior, se requiere licencia adicional para OIDC y SAML2)*
2. Posibilidad de que el usuario cambie su contraseña.
3. Comunicaciones encriptadas para todas las transacciones.
4. Impresión de informes y exportación a un archivo CSV.
5. Control de Acceso.
    a. Tarjetahabiente y grupo (agregar/modificar/borrar)
    b. Administración de credenciales (agregar/modificar/eliminar)
    c. Administración de reglas de acceso (agregar/modificar/eliminar)
    d. Administración de visitantes (registro de entrada/modificación/registro de salida)
    e. Desbloqueo de puerta
    f. Anulación del horario de desbloqueo de una puerta
    g. Informe de Actividades de Puertas
6. Alarmas.
    a. Informe de alarmas
7. Administración de los Niveles de Amenaza.
8. Reconocimiento Automático de Placas de Matrícula (ALPR).
    a. Monitoreo en vivo de las cámaras ALPR
    b. Informe de lecturas y aciertos de ALPR
    c. Registro de números de placas de matrícula en listas activas

2.23 Requisitos Generales para Aplicaciones para Teléfonos Inteligentes y Tabletas

A. La USP deberá soportar aplicaciones móviles para diferentes dispositivos disponibles en el mercado. Las aplicaciones móviles deberán comunicarse con la USP a través de cualquier conexión wifi o red celular.

B. Las aplicaciones móviles deberán comunicarse con la USP a través de una función del Mobile Server (MSR, por sus siglas en inglés). Toda comunicación entre las aplicaciones móviles y la MSR estará basada en el protocolo TCP/IP estándar y deberá usar la encriptación TLS con certificados digitales para proteger el canal de comunicación.

C. Los fabricantes de los dispositivos soportados incluyen (consultar las especificaciones de aplicaciones móviles para ver la lista de compatibilidad más reciente):

   1. Dispositivos Apple con iOS 11.0 o más reciente
   2. Dispositivos con Android 6.0 o más reciente

D. Deberá ser posible descargar las aplicaciones móviles desde la tienda de aplicaciones Central (Apple iTunes App Store, Google Play).

E. Deberá ser posible enviar la configuración a los dispositivos móviles a través de una solución de Administración de Dispositivos Móviles como VWWare Workspace One o Microsoft Intune.

F. Funcionalidades

   1. Principales

      a. Posibilidad de iniciar y cerrar sesión en la USP con un perfil de usuario autorizado del sistema

      b. Capacidad para admitir la autenticación pasiva de un proveedor de inicio de sesión única (proveedor de identidad OpenID Connect o SAML2).

      c. Posibilidad de utilizar funciones biométricas (huella digital, identificación facial, etc.) para realizar la conexión al sistema.

      d. Posibilidad de modificar la imagen o contraseña del usuario de la Mobile app.

      e. Posibilidad de ver el Nivel de Amenaza actual del sistema.

      f. Posibilidad de modificar el Nivel de Amenaza actual del sistema.

      g. Posibilidad de ejecutar acciones activas configuradas en el perfil del usuario.

      h. Posibilidad de ver entidades de la USP:

         i. Cámeras
         ii. Puertas
         iii. Cámaras ALPR
         iv. Plugins de Mosaicos Web
         v. Planos
         vi. Secuencias de Cámaras
         vii. Macros

viii. Mapas (solo mapas geográficos) *(Especificador, se requiere licencia adicional, Plan Manager Advanced)*

i. Posibilidad de navegar por la vista jerárquica de las entidades del sistema y buscar entidades en el sistema.

2. Vídeo

a. Posibilidad de ver video en vivo y grabado en las cámaras de la USP. Se podrán ver ocho cámaras como máximo.

b. Posibilidad de ver videos en formato nativo (H.264).

c. Posibilidad de ver en paralelo video en vivo y grabado para una cámara específica.

d. Posibilidad de utilizar zoom digital en las cámaras.

e. Posibilidad de realizar acciones en las cámaras, como agregar un marcador, controlar un PTZ, controlar la función de iris/enfoque, guardar una instantánea e iniciar/detener una grabación.

f. Posibilidad de ver planos de cámaras.

g. Posibilidad de ver secuencias de cámaras.

h. Posibilidad de ejecutar un informe de eventos de cámaras.

i. Posibilidad de modificar la calidad de video de las cámaras que se muestran en la aplicación móvil.

j. Posibilidad de usar la cámara del teléfono inteligente y transmitir una secuencia de video en vivo a una grabadora de video del sistema

3. Control de Acceso

a. Posibilidad de ver el estado de la puerta y de la cerradura de la puerta.

b. Posibilidad de realizar acciones en una puerta, como desbloquearla, cambiar el modo a modo de mantenimiento y anular el horario de desbloqueo.

4. Reconocimiento Automático de Placas de Matrícula

a. Posibilidad de ver eventos en vivo de una cámara ALPR.

b. Posibilidad de ver la imagen de lectura, la imagen contextual y todos los metadatos que captura la cámara ALPR.

c. Posibilidad de ejecutar un informe de eventos ALPR.

d. Posibilidad de agregar una placa de matrícula a una lista activa del sistema.

5. Administración de alarmas

a. Posibilidad de recibir notificaciones push para notificar a los operadores móviles de la recepción de una alarma.

b. Posibilidad de ver todas las alarmas activas asignadas al operador móvil.

c. Posibilidad de realizar acciones en una alarma, como reconocer, reenviar o alternar el reconocimiento de una alarma activa.

d. Posibilidad de ver entidades vinculadas a la alarma.

6. Mapas *(Especificador, se requiere licencia adicional, Plan Manager Advanced)*

a. Posibilidad de ver mapas geográficos con entidades de la USP localizadas geográficamente en el mapa.

b. Posibilidad de ver cualquier entidad configurada en el mapa.

c. Posibilidad de ir a ubicaciones de mapas predefinidas mediante botones predeterminados.

d. Posibilidad de buscar entidades o ubicaciones en el mapa.

7. Administración de incidentes

a. Capacidad para ver incidentes activos, ordenarlos y agruparlos para una vista personalizada.

b. Capacidad para disparar incidentes de forma manual.

c. Capacidad para obtener todos los detalles sobre un incidente, incluidos los incidentes, las entidades y los documentos relacionados.

d. Capacidad para apropiarse de un incidente y responder al procedimiento operativo estándar definido orientado a la resolución de incidentes.

G. Posibilidad de enviar un mensaje desde la interfaz del usuario de clientes a un operador móvil.

H. Posibilidad de enviar una secuencia de video en vivo o grabada desde la interfaz del cliente a un operador móvil.

I. Posibilidad de ver los operadores móviles que hayan habilitado el rastreo de ubicación en un mapa del sistema. La ubicación del operador móvil debería actualizarse en tiempo real. *(Especificador, Plan Manager Advanced, se requiere licencia adicional)*

2.24 Monitor de salud

A. La USP deberá monitorear el estado de salud del sistema, los eventos relacionados con los registros del estado de salud y calcular estadísticas.

B. Los servicios de la USP, funciones, agentes, unidades y aplicaciones de clientes activarán los eventos de los estados de salud.

C. La USP deberá llenar el Registro de Eventos Windows con eventos del estado de salud relacionados con las funciones de la USP, servicios y aplicaciones de clientes.

D. Una función exclusiva, la Función de Monitoreo del Estado de Salud, deberá realizar las siguientes acciones:

   1. Monitorear el estado de la salud de todo el sistema y los eventos de registros.
   2. Calcular estadísticas dentro de un marco de tiempo específico (horas, días, meses).
   3. Calcular la disponibilidad para los clientes, servidores y unidades de videos/acceso/ALPR.

E. Una tarea de Monitoreo del Estado de Salud y una tarea de generación de informes del Historial del Estado de Salud deberá estar disponible para la generación de informes en vivo y de historiales.

F. En la interfaz de usuario de la aplicación cliente, una tarea del tablero de control correspondiente al Monitoreo del Estado de Salud para proporcionar información en vivo, como gráficos circulares y listas de eventos, con el objetivo de evaluar de forma rápida y visual la salud general del sistema.

G. Un tablero de control del estado de salud centralizado basado en la web deberá estar disponible para visualizar las unidades y eventos de funciones del estado de salud de la USP de manera remota.

H. Estadísticas detalladas del cuidado del sistema estarán disponibles a través de un tablero de control basado en la web, y proporcionará métricas del estado de salud de las entidades y funciones de la USP, incluyendo tiempo activo y tiempo promedio entre fallas.

I. Todos los eventos de salud generados en el sistema se pueden usar para automatizar la administración de eventos y acciones de la USP.

J. Los eventos del estado de salud serán accesibles a través del SDK (puede usarse para crear capturas de SNMP).

2.25 Requisitos Generales de la USP

A. La Plataforma Unificada de Seguridad (USP) deberá ser una solución de software clase empresarial de seguridad y protección habilitada para IP.

B. La USP deberá soportar la unificación transparente del Sistema de Control de Acceso IP (ACS), el Sistema de Administración de Videos IP (VMS), y el Sistema de Reconocimiento Automático de Placas de Matrícula IP (ALPR) bajo una sola plataforma. Las aplicaciones de interfaz de usuario (UI, por sus siglas en inglés) de la USP deberán presentar una interfaz de seguridad unificada para la administración, la configuración, el monitoreo y la generación de informes de los sistemas incrustados ACS, VMS y ALPR, y dispositivos periféricos asociados.

C. Las funcionalidades disponibles con la USP deberán incluir:

   1. La configuración de sistemas embebidos, como los sistemas ACS, ALPR y VMS.
   2. El monitoreo de eventos en vivo.

3. El monitoreo de video en vivo y reproducción de video archivado.
4. Administración de alarmas.
5. La generación de informes que incluyan la creación de plantillas de informes personalizados e informes de incidentes.
6. La característica de Federation™ para el monitoreo global, la generación de informes y la administración de alarmas de múltiples sistemas ACS, VMS y/o ALPR remotos e independientes esparcidos a lo largo de múltiples instalaciones y zonas geográficas. *(Especificador, solo Enterprise, se requiere licencia adicional)*
7. La administración global de tarjetahabientes a lo largo de múltiples instalaciones y zonas geográficas, cada una con su propio sistema ACS independiente. *(Especificador, solo Enterprise, se requiere licencia adicional para cada sitio)*
8. Integración de Microsoft Active Directory para la sincronización de las cuentas de usuarios de la USP y cuentas de tarjetahabientes del ACS. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
9. Dispositivo de intrusión e integración de paneles (monitoreo en vivo, generación de informes y armado/desarmado). *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
10. Integración de los dispositivos de Intercomunicador SIP para comunicación bidireccional. *(Especificador, todas las versiones, se requiere licencia adicional)*
11. Integración con sistemas y bases de datos de terceros a través de plug-ins (control de acceso, analíticas de video, puntos de venta, y otros.). *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
12. Visualización de mapas gráficos dinámicos.
13. Integración del sistema de administración de activos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

D. La USP deberá ser instalada en uno o más de los siguientes tipos de instalaciones:

1. Acceso unificado, ALPR, plataforma de videos y cualquier combinación de los mismos.
2. Control de acceso independiente, video o plataforma ALPR.
3. Acceso unificado y plataforma de video que federa con múltiples ACS, VMS y ALPR remotos.
4. Control de acceso independiente que federa múltiples ACS remotos independientes.

E. Concesión de licencias:

1. Se deberá aplicar una sola concesión de licencias central en el servidor de configuración.

2. No deberá existir un requisito de aplicar una licencia en todo servidor de computadora o estación de trabajo de cliente.

3. Con base en las opciones seleccionadas, se podrán habilitar o deshabilitar uno o más sistemas embebidos.

F. Requisitos de Hardware y Software:

1. Los sistemas de la USP y los embebidos (video, reconocimiento de placas de matrícula y control de acceso) deberán estar diseñados para ejecutarse sobre una plataforma estándar basada en PC equipada con el sistema operativo Windows. El sistema operativo preferido deberá ser coordinado con el Propietario siguiendo los sistemas operativos soportados por el fabricante.

2. El software básico del cliente/servidor será desarrollado en su totalidad usando la plataforma de software .NET de Microsoft y el lenguaje de programación C# (C-Sharp).

3. El(los) servidor(es) de base de datos de la USP deberá(n) estar desarrollado(s) sobre el Servidor SQL de Microsoft. La versión SQL preferida deberá coordinarse con el Propietario y ser compatible con la USP.

4. La USP deberá ser compatible con los ambientes virtuales, incluyendo VMware y Microsoft Hyper-V.

5. La USP deberá usar el desarrollo y las tecnologías de programación más recientes de interfaz de usuario (UI) como lo son Microsoft WPF (Windows Presentation Foundation), el lenguaje de marcado XAML, y la plataforma de software .NET.

2.26 Arquitectura de la USP

A. La USP estará basada en un modelo de cliente/servidor. La USP deberá consistir de un Módulo de Software de Servidor (SSM) estándar y Aplicaciones de Software del Cliente (CSA).

B. La USP deberá ser una solución habilitada para IP. Toda la comunicación entre el SSM y la CSA estará basada en el protocolo TCP/IP estándar y deberá usar la encriptación TLS con certificados digitales para proteger el canal de comunicación.

C. El SSM deberá ser un servicio Windows que se pueda configurar para que comience a funcionar cuando se inicia y ejecuta el sistema operativo en el fondo. El SSM deberá comenzar a funcionar automáticamente cuando se enciende la computadora sin importar si hay o no un usuario con sesión iniciada en la máquina.

D. Los usuarios podrán implementar el SSM en un solo servidor o a lo largo de varios servidores para una arquitectura distribuida. La USP no tendrá restricciones en cuanto al número de SSM instalados.

E. La USP deberá soportar el concepto de la característica de Federation en donde se pueden enlazar múltiples instalaciones independientes ACS, VMS y ALPR en un solo sistema virtual grande para el monitoreo, generación de informes y gestión de alarmas centralizados. *(Especificador, solo Enterprise, se requiere licencia adicional)*

F. La USP deberá proteger contra la posible falla del servidor de la base de datos y continuar funcionando con soluciones estándar disponibles en el mercado .

G. La USP deberá soportar hasta mil instancias de CSA conectadas al mismo tiempo. Sin embargo, se puede instalar un número ilimitado de CSA en cualquier momento. *(Especificador, máximo 5 con Standard; máximo 10 con Professional; ilimitado con Enterprise)*

H. La USP deberá soportar un número ilimitado de registros e historial de transacciones (eventos y alarmas) con el máximo permitido limitado por la cantidad de disco duro disponible.

I. Arquitectura con Base en Funciones:

1. La USP deberá consistir de una arquitectura con base en funciones, donde cada SSM hospeda una o más funciones.
2. Cada función deberá ejecutar un conjunto específico de tareas relacionadas al sistema principal, el reconocimiento automático de placas de matrícula automotriz (ALPR), videos (VMS) o funcionalidades de control de acceso (ACS), entre muchas otras más. La instalación deberá estar simplificada a través de la habilidad de la USP para permitir a los administradores:
    a. Instalar uno o varios SSM a lo largo de la red antes de activar las funciones.
    b. Activar y desactivar funciones según sea necesario en todos y cada uno de los SSM.
    c. Centralizar la configuración y administración de la función.
    d. Soporte de configuración remota.
    e. Mover las funciones desde un SSM a otro.
3. Cada función, cuando sea necesario, deberá tener su propia base de datos para almacenar eventos e información de configuración específica a la función.
4. Las funciones sin base de datos, como la característica de Federation, Active Directory, y Administración Global de Tarjetahabientes, deberán soportar el modo de espera muy próximo al tiempo real sin que se requiera software de conmutación por error de terceros.
5. Función del Directory:
    a. La Función de Directory deberá administrar la base de datos central que contiene toda la información del sistema y la configuración de componentes de la USP.
    b. La Función de Directory deberá autenticar usuarios y dar acceso a la USP con base en derechos o privilegios de acceso predefinidos del usuario y configuraciones de particiones de seguridad.

c. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes comunes a los subsistemas del ACS, ALPR y el VMS:
    i. Particiones de seguridad, usuarios y grupos de usuarios
    ii. Áreas
    iii. Zonas, reglas de enlace de entrada/salida (E/S) y comportamiento de salida personalizado
    iv. Alarmas. Horarios y tareas programadas
    v. Eventos personalizados
    vi. Macros o guiones personalizados
d. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al VMS:
    i. Servidores de video y sus periféricos (como audio, E/S y puertos serie)
    ii. PTZ.
    iii. Secuencias de cámaras
    iv. Horarios de grabación y archivamiento
e. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al ACS:
    i. Controladores de puertas, y módulos de entrada y salida (E/S)
    ii. Puertas, Elevadores y Reglas de acceso
    iii. Tarjetahabientes y grupos de tarjetahabientes, credenciales y plantillas para distintivos
f. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al ALPR:
    i. Unidades y cámaras ALPR
    ii. Listas activas, listas de permisos y reglas de sobretiempo

6. La Función del Video Archiver será responsable de administrar las cámaras y los codificadores que controle y archive.
7. La Función del Media Router será responsable de enrutar los flujos de video y audio en redes locales y de área extensa, desde la fuente (como el DVS) hacia el destino (como la CSA).
8. La Función del Administrador de Acceso será responsable de la sincronización de las unidades de hardware de control de acceso bajo su control, como lo son los controladores de puerta y los módulos de E/S. Además esta función debe ser responsable de validar y registrar todas las actividades y eventos de acceso cuando los controladores de puertas y los módulos E/S están en línea.

9. La Función del Reconocimiento Automático de Placas de Matrícula (ALPR) será responsable de sincronizar las unidades fijas ALPR (cámaras) y aplicaciones ALPR móviles bajo su control. La Función de ALPR será responsable de registrar todas las actividades y eventos del ALPR.
10. La Función de Zone Manager será responsable de administrar todas las zonas de software (recopilación de entradas) y el registro de eventos de zona asociados. Las zonas deberán consistir de entradas de control de acceso y de dispositivos de video.
11. La Función de Monitoreo del Estado de Salud será responsable por el monitoreo y registro de eventos y advertencias del estado de salud desde varias aplicaciones de cliente, funciones, y servicios que forman parte de la USP. Esta función también será responsable de registrar eventos dentro del Windows Event Log y por generar informes sobre las estadísticas y el historial de salud.
12. La función de ingestión de datos será responsable de ingerir datos de fuentes externas para mejorar las capacidades de generación de informes y tableros de control del sistema.
13. Funciones Opcionales
    a. La Característica de Federation™ será responsable de crear un gran sistema virtual que consista de cientos o miles de sistemas ACS, VMS y/o ALPR independientes y remotos. *(Especificador, solo Enterprise, se requiere licencia adicional)*
    b. La Función del Global Cardholder Synchronizer será responsable de sincronizar la información de los tarjetahabiente y credenciales entre el sitio local y el sitio central. También deberá soportar la sincronización entre sitios remotos. *(Especificador, solo Enterprise, se requiere licencia adicional)*
    c. La Función del Active Directory será responsable de sincronizar las cuentas de los usuarios y cuentas de los tarjetahabientes con un servidor Microsoft Active Directory. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
    d. La Función del Intrusion Manager será responsable de administrar los dispositivos de intrusión de terceros como los paneles de alarmas y dispositivos de detección de perímetros. Esta función también será responsable de registrar de todos los eventos de intrusión en una base de datos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
    e. La Función del Asset Manager será responsable de integrar y sincronizar los sistemas de administración de activos de terceros y eventos relacionados con el registro de activos. La función será responsable de soportar la ejecución de informes relacionados con activos como informes de inventarios e informes de actividad de activos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
    f. El Rol de Plugin Manager deberá ser responsable por la comunicación entre la USP y los sistemas de terceras partes como lo son datos analíticos de

video, los sistemas de control de acceso y video, los ALPR y los sistemas de gestión de edificios. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

g. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

h. La Función de Web SDK será responsable de conectar la USP a cualquier aplicación o interfaz desarrollada con el Web Service SDK. Las aplicaciones desarrolladas con el Web Service SDK serán independientes de la plataforma y dependerán del protocolo REST para las comunicaciones. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

i. La Función Communication Management será responsable de registrar los extremos de comunicación SIP y por administrar el enrutamiento de las llamadas. *(Especificador, todos los paquetes, se requiere licencia adicional)*

J. Servicio de Monitoreo de Servidores (Watchdog):

1. La USP deberá incluir un Servicio de Monitoreo de Servidores que monitoree continuamente el estado del servicio del Módulo de Software del Servidor (SSM).

2. El Servicio de Monitoreo de Servidores será un servicio Windows que se inicia de forma automática en el encender el sistema, sin importar si el usuario está conectado o no a su cuenta.

3. El Servicio de Monitoreo de Servidores estará instalado en todos los servidores y PC que ejecutan un SSM. En caso de fallas o funcionamiento defectuoso, el Servicio de Monitoreo de Servidores deberá reiniciar el servicio averiado. Como último recurso, el Servicio de Monitoreo de Servidores deberá reiniciar el servidor/PC si no fuera posible reiniciar el servicio.

2.27 Control de acceso USP, video y unificación ALPR

A. El Monitoreo UI deberá presentar una verdadera Interfaz de Seguridad Unificada para el monitoreo y los informes en vivo del ACS, el VMS y el ALPR. La visualización y reproducción avanzada de vídeo en vivo de vídeo archivado deberá estar disponible a través de la UI de Monitoreo.

B. La configuración de UI deberá presentar una verdadera Interfaz de Seguridad Unificada para la configuración y administración del ACS, el VMS y el ALPR.

C. El usuario deberá ser capaz de asociar una o más cámaras de video a los siguientes tipos de entidad: áreas, puertas, elevadores, zonas, alarmas, paneles de intrusión, cámaras ALPR y más.

D. Será posible ver el video asociado con los eventos de control de acceso cuando se visualiza un informe.

E. Será posible ver el video asociado con los eventos de los paneles de intrusión cuando se visualiza un informe.

F. Deberá ser posible ver el video asociado con los eventos del ALPR cuando se visualice un informe.

2.28 Administración de Alarmas de la USP

A. La USP deberá soportar la siguiente funcionalidad de la Administración de Alarmas:

1. Crear y modificar alarmas definidas por el usuario. Deberá soportar un número ilimitado de alarmas definidas por el usuario.
2. Asignar un cronograma de tiempo o período de cobertura a una alarma. Deberá activarse una alarma solamente si es una alarma válida para el período de tiempo actual.
3. Establecer el nivel de prioridad de una alarma y su umbral de reactivación.
4. Definir si se visualiza video en vivo o grabado, imágenes fijas o una mezcla de estos una vez que se activa una alarma.
5. Proporcionar la habilidad de visualizar video en vivo y grabado dentro del mismo recuadro de video utilizando el modo imagen en imagen (PiP).
6. Proporcionar la habilidad de agrupar alarmas por fuente y por tipo.
7. Definir un período de tiempo después del cual se reconoce de forma automática la alarma.
8. Definir los destinatarios de una alarma. Las notificaciones de alarmas deberán distribuirse a uno o más destinatarios. Los destinatarios deberán recibir un nivel de prioridad que jerarquice el orden de recepción de una alarma.
9. Definir el modo de transmisión de la alarma. Las notificaciones de alarmas se enviarán usando un modo de transmisión secuencial o un modo de transmisión de todo a la vez.
10. Definir si se visualiza la fuente de la alarma, una o más entidades o una página HTML.
11. Especificar si es obligatorio la generación de un informe de incidente durante el reconocimiento.

B. Los flujos de trabajo para crear, modificar, agregar instrucciones y procedimientos, y reconocer una alarma deberán ser consistentes para las alarmas de control de acceso, ALPR y videos.

C. Las alarmas estarán federadas, lo que permitirá la administración global de alarmas a lo largo de múltiples sistemas independientes USP, ACS y VMS.

D. La USP deberá además soportar la notificación de alarmas a una dirección de correo electrónico o a cualquier dispositivo que usa el protocolo SMTP.

E. La habilidad para crear instrucciones relacionadas con las alarmas será soportada a través de la visualización de una o más páginas HTML después de un evento de

alarma. Las páginas HTML deberán ser definidas por el usuario y se podrán vincular entre sí.

F. Deberá soportarse el empaque y desempaque de la alarma en donde todas las entidades relacionadas con una alarma se puedan visualizar en la UI de Monitoreo con un simple clic de un botón.

G. El usuario tendrá la habilidad de reconocer alarmas, crear un incidente al reconocer una alarma, y colocar una alarma en el modo repetición.

H. El usuario deberá ser capaz de activar alarmas de forma espontánea con base a lo que vea en el sistema.

I. Una alarma deberá estar configurada de tal forma que permanezca visible hasta que se reconozca la condición de la fuente.

J. El usuario será capaz de investigar la alarma sin tener que reconocerla.

2.29 Niveles de amenaza de la USP *(Especificador: se requiere licencia adicional; solo Enterprise)*

A. La USP deberá soportar los Niveles de Amenaza para cambiar de forma dinámica el comportamiento del sistema para responder a eventos críticos.

B. Los Niveles de Amenaza deberán activarse y desactivarse por el operador de la CSA con el privilegio adecuado.

C. Los Niveles de Amenaza deberán establecerse en un área o en todo el sistema.

D. Los Niveles de Amenaza afectarán el comportamiento del sistema al ejecutar cualquier acción disponible en la USP, como: activar salida, iniciar la grabación, bloquear cámaras, invalidar la calidad de la grabación, armar una zona, colocar una puerta en un modo de mantenimiento, y otros.

E. Deberán estar disponibles las siguientes acciones específicas con los Niveles de Amenaza:

1. Establecer una autorización de seguridad mínima para restringir o permitir el acceso de tarjetahabientes a áreas específicas además de otras restricciones impuestas por las reglas de acceso.

2. Establecer un nivel de usuario mínimo para cerrar automáticamente la sesión del usuario en la USP.

3. Establecer el modo de lector para cambiar la forma de obtener acceso a las puertas (por ejemplo, tarjeta y PIN, o tarjeta o PIN).

F. Se deberá visualizar una notificación visible en toda la CSA del operador cuando se active un Nivel de Amenaza.

2.30 Administración Avanzada de Tareas de la USP

A. La USP deberá soportar una infraestructura para administrar las tareas de la UI de Monitoreo que se usan para el monitoreo en vivo, las actividades diarias y la generación de informes.

B. Los administradores deberán ser capaces de asignar tareas y bloquear el área de trabajo del operador. La administración del usuario de su área de trabajo deberá estar limitada por sus privilegios asignados.

C. Los operadores deberán ser capaces de guardar sus tareas, ya sea como tareas Públicas o tareas Privadas, y en una partición específica. Las Tareas Públicas deberán estar disponibles para todos los usuarios. Las Tareas Privadas solo deberán estar disponibles para el propietario de la tarea.

D. Los operadores deberán ser capaces de compartir sus tareas enviándolas a uno o más usuarios en línea. Los destinatarios deberán tener la opción de aceptar la tarea enviada.

E. Los operadores deberán ser capaces de duplicar una tarea.

2.31 Informes de la USP

A. La USP deberá soportar la generación de informes (informes de base de datos) para el control de acceso, ALPR, videos e intrusión.

B. Todos y cada uno de los informes en el sistema deberá ser una tarea de la USP, cada una asociada con su propio privilegio. Un usuario deberá tener acceso a una determinada tarea de informe si cuenta con los privilegios correspondientes.

C. Los flujos de trabajo para crear, modificar, y ejecutar un informe deberán ser consistentes para los informes de control de acceso, ALPR y video.

D. Los informes deberán ser federados, lo que permite la generación de informes globales consolidados a lo largo de múltiples sistemas independientes USP, ACS, VMS y ALPR.

E. Los informes de control de acceso y ALPR deberán soportar las fotos de los tarjetahabientes y fotos de las placas de matrícula, respectivamente.

F. La USP deberá soportar los siguientes tipos de informes:

1. Informes de alarmas
2. Informes específicos de video (archivos, marcadores, movimiento y otros)
3. Informes de configuración (tarjetahabientes, credenciales, unidades, reglas de acceso, lectores/entradas/salidas y más)
4. Informes de actividades (tarjetahabientes, grupo de tarjetahabientes, visitantes, credenciales, puertas, unidades, áreas, zonas, elevadores y más)

5. Informes específicos de ALPR (reproducción de ALPR móvil, aciertos, lecturas de placas, lecturas/aciertos por día, lecturas/aciertos por zona de ALPR y demás)
6. Informes de actividad del estado de salud y estadísticas del estado de salud
7. Otros tipos de informes, como informes de visitantes, informes de registros de auditoría, informes de incidentes e informes de horario y asistencia

G. Informes Genéricos, Informes Personalizados y Plantillas de Informes:

1. El usuario deberá tener la opción de generar informes genéricos desde una lista existente, generar informes desde una lista de plantillas definidas por el usuario, o crear un nuevo informe o una plantilla de informe.
2. El usuario deberé ser capaz de personalizar informes predefinidos y guardarlos como nuevas plantillas de informe. No existirá la necesidad de una herramienta externa de generación de informes para crear informes personalizados y plantillas de informe. Las opciones de personalización incluirán la configuración de filtros, extensión del informe, y período de tiempo de espera. El usuario también deberá ser capaz de establecer cuales columnas serán visibles en un informe. La clasificación de los datos reportados estará disponible haciendo clic en la columna correspondiente y seleccionando un criterio de clasificación (ascendente o descendente).
3. Todas las plantillas de informes deberán crearse dentro de la UI de Monitoreo.
4. Estas plantillas se pueden usar para generar informes sobre un cronograma en formato PDF o Excel.
5. Un número ilimitado de informes y plantillas personalizadas serán soportados.

H. El diagrama de una tarea de generación de informes deberá consistir de paneles con configuraciones (duración de informe, filtros, mandos ‘ir a’ y ‘restablecer’, etc.), los datos actuales del informe en formato de columna, y un panel con recuadros de visualización. El usuario deberá ser capaz de arrastrar y soltar registros individuales en un informe sobre uno o más recuadros de visualización para ver la foto de identificación de un tarjetahabiente, reproducir una secuencia de video, o un evento ALPR.

I. La USP deberá soportar el filtrado completo de datos para la mayoría de los informes con base en el tipo de entidad, tipo de evento, marca de tiempo del evento, campos personalizados, etc.

J. La tarea de informe tendrá la capacidad de mostrar resultados a través de gráficos, como gráficos de líneas, gráficos de barras, gráficos de barras apiladas, gráficos de anillos y gráficos circulares.

K. El usuario deberá ser capaz de hacer clic sobre una entidad dentro de un informe existente para generar informes adicionales desde la UI de Monitoreo.

L. La USP deberá soportar las siguientes acciones en un informe: imprimir el informe, exportar el informe a un archivo PDF/Microsoft Excel/CSV, exportar los gráficos en

formato JPG/PNG y enviar de manera automática por correo electrónico un informe en función de un horario y una lista de uno o más destinatarios.

2.32 Tableros de la USP

A. La USP deberá ser capaz de crear tableros.

B. Los operadores deberán poder ver los tableros si cuentan con los privilegios correspondientes. Los usuarios con los privilegios correspondientes también deberán ser capaces de modificar los tableros.

C. Los tableros del sistema deberán ser una tarea de la USP. Un usuario deberá tener acceso a una tarea específica de tablero si cuenta con los privilegios correspondientes.

D. Los tableros se deberán guardar en una carpeta privada o pública.

E. Un tablero deberá estar formado por un área de trabajo con varios widgets que aparezcan en dicha área. Todos los widgets deberán proporcionar la capacidad de especificar su ubicación y tamaño, un título y un color de fondo, y de ofrecer la capacidad de actualizar su contenido con frecuencia.

F. Tipos de widgets para tableros:

1. Imagen: ofrece la capacidad de mostrar una imagen (JPG, PNG, GIF y BMP) en un tablero.

2. Texto: ofrece la capacidad de mostrar texto en un tablero. El estilo del texto deberá poder configurarse, de manera que el usuario pueda especificar la fuente, el tamaño, el color y la alineación.

3. Mosaico: ofrece la capacidad de mostrar cualquier entidad de la USP en un mosaico.

4. Página web: ofrece la capacidad de mostrar una URL en un tablero.

5. Cantidad de entidades: ofrece la capacidad de mostrar la cantidad total de un determinado tipo de entidad en la USP.

6. Informes: ofrece la capacidad de mostrar los resultados de los informes guardados en el sistema. Los resultados se visualizarán mostrando la cantidad total de resultados en el informe, un conjunto de los principales resultados del informe o un gráfico visual de los datos del informe.

G. Será posible ampliar los widgets de un tablero con un SDK. De esta forma, se podrán desarrollar widgets personalizados para el sistema.

H. La USP deberá soportar las siguientes acciones en un tablero: imprimir el tablero, exportar el tablero a un archivo PNG y enviar automáticamente por correo electrónico un informe en función de un horario y una lista de uno o más destinatarios.

2.33 Característica de Federation de la USP: Monitoreo de sistemas remotos *(Especificador: solo Enterprise, licencia adicional obligatoria para cada sitio y entidad federada.)*

A. La USP deberá soportar el concepto de una función federada para el control de acceso, video y ALPR.

B. La característica de Federation permitirá la unificación de múltiples sistemas USP independientes (sistemas Federados) en un solo sistema virtual más grande (la característica de Federation). Esto deberá facilitar el monitoreo global de múltiples sistemas USP independientes.

C. La característica de Federation deberá soportar la unificación de múltiples sistemas independientes de videovigilancia o VMS.

D. La característica de Federation deberá soportar la unificación de múltiples sistemas independientes de control de acceso o ACS.

E. La característica de Federation deberá soportar la unificación de múltiples sistemas independientes de reconocimiento de placas de matrícula vehicular ALPR.

F. Las entidades que se federarán y monitorearán de forma centralizada desde la característica de Federation deberán incluir alarmas, áreas, cámaras, tarjetahabientes y grupos de configuración de tarjetahabientes, credenciales, puertas, elevadores, eventos ALPR y zonas (entradas monitoreadas).

G. La característica de Federation deberá soportar una integración basada en nube, por medio de la cual se actualizarán de forma automática el servicio e infraestructura y la proporcionará el proveedor del servicio, sin la necesidad de hardware en el sitio.

H. La característica de Federación deberá soportar la Gestión Global de Alarmas, desde el monitoreo de UI para el control de acceso, video y ALPR.

I. La función de federación deberá soportar la Generación Global de Informes desde el monitoreo de UI para el control de acceso, video y ALPR.

J. La característica de Federation deberá soportar docenas de acciones del operador en entidades remotas (federadas) desde la UI de Monitoreo (por ejemplo, generar un informe global tomando en cuenta eventos de múltiples sitios independientes o reconocer alarmas remotas).

2.34 Administración de Zonas de la USP

A. La USP deberá soportar la configuración y administración de las zonas para el monitoreo del punto de entrada a través de la Función del Zone Manager. Un usuario podrá agregar, borrar o modificar una zona si cuenta con los privilegios correspondientes.

B. Una zona deberá monitorear el estado de uno o más puntos de entrada. Deberá ser posible el monitoreo de la zona o de un punto de entrada a través del uso de un controlador y uno o más módulos de entrada. Las entradas desde las cámaras o codificadores de video también deberán estar accesibles a través de una zona.

C. Dependiendo del hardware que está instalado deberán soportarse las entradas supervisadas. Dependiendo del módulo de entrada usado se deberá tener disponibilidad de supervisión tanto de 3 como de 4 estados.

D. Se deberá definir un cronograma para una zona indicando cuándo se monitoreará la zona.

E. Los Eventos Personalizados deberán ofrecer una flexibilidad completa para crear eventos personalizados específicos a una zona. El usuario será capaz de asociar los eventos personalizados a los cambios de estado en las entradas monitoreadas.

F. El ACS deberá soportar una o más cámaras por zona. Videos deberán estar asociados a los cambios de estado de una zona.

G. Vincular Entrada/Salida (E/S)

1. La administración de las zonas deberá soportar la Vinculación de Entrada/Salida (E/S). La Vinculación de E/S deberá permitir que una o más entradas activen una o más salidas.

2. La Vinculación de E/S deberá estar disponible en el modo fuera de línea cuando la comunicación entre el servidor y el hardware no está disponible.

3. Los Comportamientos de Salida Personalizados deberán ofrecer completa flexibilidad para crear una variedad de patrones complejos de señal de salida: pulsos simples, pulsos periódicos, pulsos de ciclo variable, y cambios de estado.

4. A través de la acción de 'activación de salida', el ACS deberá soportar la activación de salidas con comportamientos de salida personalizados.

2.35 Administración de Seguridad del Usuario y Grupo de Usuarios, Particiones y Privilegios de la USP

A. La USP deberá soportar la configuración y la administración de usuarios y grupos de usuarios. Un usuario podrá agregar, borrar o modificar un usuario o grupo de usuarios si cuenta con los privilegios correspondientes.

B. La USP deberá soportar la autenticación de usuario con autenticación basada en notificaciones usando proveedores externos. Los proveedores externos deberán incluir:

1. ADFS (Servicios de federación de Active Directory)

2. Azure Active Directory (a través de OpenID Connect)

3. Ping Identity (a través de OpenID Connect)

4. KeyCloak (a través de OpenID Connect)

5. Otros agentes de autenticación de Open ID Connect/SAML2

C. Los derechos y privilegios de acceso comunes compartidos por múltiples usuarios deberán definirse como Grupos de Usuarios. Los miembros individuales del grupo

deberán heredar los derechos y privilegios de sus grupos de usuarios primario. Se permitirá el anidamiento de grupo de usuarios.

D. Los privilegios del usuario deberán ser amplios en la USP. Todas las entidades configurables para la USP, incluyendo el control de acceso, video y ALPR, deberán contar con privilegios asociados.

E. Las entidades específicas, como tarjetahabientes, grupos de tarjetahabientes, y credenciales, deberán incluir un juego de privilegios más pormenorizado, como el derecho al acceso a campos personalizados y cambio de activación o estado del perfil de una entidad.

F. Particiones:

1. La USP deberá limitar lo que pueden ver los usuarios en la base de datos de configuración a través de particiones de seguridad (segmentos de base de datos). El administrador, quien cuenta con todos los derechos y privilegios, tendrá permitido segmentar un sistema en múltiples particiones de seguridad.

2. Todas las entidades que forman parte de la USP se pueden asignar a una o más particiones.

3. Un usuario que reciba acceso a una partición específica solo deberá ser capaz de ver las entidades (componentes) dentro de la partición a la cuál ha sido asignado. El acceso se otorga al asignar al usuario como un usuario aceptado para ver las entidades que forman parte de una partición en particular.

4. Un usuario o grupo de usuarios puede recibir derechos de administrador sobre la partición.

G. Deberá ser posible especificar el usuario y los privilegios del grupo de usuarios con base en la partición.

H. Las opciones avanzadas de inicio de sesión deberán estar disponibles como inicio de sesión doble, y otros.

I. Deberá ser posible especificar un período inactivo para la UI de Monitoreo y después de dicho tiempo la aplicación se bloqueará de forma automática, al mismo tiempo que conserva el acceso a las señales de la cámara visualizadas actualmente.

J. Será posible revisar los permisos de los usuarios y determinar lo siguiente:

1. El usuario o grupo de usuarios que pueden ver o modificar una entidad del sistema.

2. Los privilegios de cada usuario o grupo de usuarios del sistema.

3. El usuario o grupo de usuarios que puede realizar la acción vinculada a un privilegio.

2.36 Administración de evento/acción de la USP

A. La USP deberá soportar la configuración y la administración de eventos para videos y ALPR. Un usuario será capaz de agregar, eliminar o modificar una acción enlazada a un evento si cuenta con los privilegios correspondientes.

B. La USP deberá recibir todos los eventos entrantes desde uno o más ACS, VMS y/o ALPR. La USP deberá tomar las acciones correspondientes con base a relaciones de eventos/acciones definidas por el usuario.

C. La USP deberá recibir y registrar los siguientes eventos:

1. Eventos en todo el sistema
2. Eventos de aplicación (clientes y servidores)
3. Eventos de áreas, cámaras, puertas, elevadores y ALPR (lecturas y aciertos)
4. Eventos de tarjetahabientes y credenciales
5. Eventos de unidad
6. Eventos de zona
7. Eventos de alarmas
8. Eventos ALPR
9. Eventos de primera persona que entra y última persona que sale y eventos de anti-retorno (anti-passback)
10. Eventos de intrusión
11. Eventos de gestión de activos
12. Eventos de monitoreo del estado de salud.

D. La USP deberé permitir la creación de eventos personalizados.

E. La USP deberá contar con la capacidad para ejecutar una acción en respuesta a un evento de control de acceso, video y ALPR.

F. La USP deberá permitir que un cronograma se asocie con una acción. Deberá activarse la acción solamente si es una acción adecuada para el período de tiempo actual.

2.37 Programas y tareas programadas de la USP

A. Programaciones

1. La USP deberá soportar la configuración y la administración de cronogramas complejos. Un usuario podrá agregar, borrar o modificar un horario si cuenta con los privilegios correspondientes.

2. La USP deberá ofrecer total flexibilidad y la capacidad de detallar cuando se crea un cronograma. El usuario deberá ser capaz de definir un cronograma en incrementos de 1 o 15 minutos.

3. Deberán soportarse programas diarios, mensuales, ordinales y específicos.

B. Tareas Programadas

1. La USP deberá soportar tareas programadas para el control de acceso, video y ALPR.

2. Las tareas programadas deberán ejecutarse sobre un cronograma definido por el usuario en un día y hora específico. También deberá soportar tareas periódicas o recurrentes bajo un cronograma.

3. Las tareas programadas deberán soportar todas las acciones estándar disponibles dentro de la USP, como enviar un correo electrónico o enviar un informe por correo electrónico.

2.38 Macros y Scripts Personalizados de la USP

A. La USP deberá habilitar a los usuarios a automatizar y ampliar las funcionalidades del sistema a través del uso de macros o scripts personalizados para el control de acceso, video y ALPR.

B. Los macros personalizados deberán crearse con el Kit de Desarrollo de Software (SDK) de la USP.

C. Una macro deberé ejecutarse tanto de forma automática como manual.

D. Se deberá lanzar una macro en la UI de Monitoreo a través de acciones activas.

2.39 Mapas gráficos dinámicos (DGM) de la USP

A. La USP deberá soportar la funcionalidad de mapeo para el control de acceso, videovigilancia, detección de intrusión, ALPR y aplicaciones externas.

B. La USP deberá proporcionar una interfaz centrada en mapas con la habilidad de comando y control de todas las capacidades de la USP desde una interfaz de mapa de pantalla completa.

C. Deberá ser posible extender el mapa sobre todas las pantallas de la estación del cliente de la USP. En el escenario en donde el mapa se extiende sobre todas las pantallas de la estación del cliente de la USP, deberá ser posible navegar el mapa incluyendo panorámica y zoom, y los movimientos del mapa deberán estar sincronizados en todas las pantallas. La expansión del mapa en varias pantallas debe ofrecer las mismas capacidades de mando y control que la visualización en una sola pantalla.

D. Los DGM deberán soportar los siguientes formatos de archivos y protocolos para la importación de los fondos mapas:

1. PDF

2. JPG
3. PNG
4. Servicio de Mosaico de Mapas Web (WMTS, por sus siglas en inglés) y Servicio de Mapas Web (WMS, por sus siglas en inglés) definidos por el Open Geospatial Consortium (OGC)
5. BeNomad
6. AutoCAD (DWG y DXF)

E. El DGM deberá proporcionar los siguientes proveedores de mapas en línea para usar como fondo de mapa y proporcionar la habilidad de administrar su licencia de servicio, si se requiere una:

1. Google Map, aéreo, topografía (Con licencia)
2. Bing Map, aéreo, satélite, híbrido (Con licencia)
3. ESRI ArcGIS (con licencia)
4. Mapa aéreo OpenStreet (con licencia)
5. OVI híbrido

F. Deberá ser posible configurar un conjunto de mapas mixtos elaborados por GIS, proveedores en línea y archivos privados importados y enlazarlos todos juntos.

G. Los DGM deberán proporcionar la habilidad de visualizar todas las entidades nativas de la USP, entre las que se incluyen:

1. Cámaras, corregir y PTZ
2. Puertas
3. Secuencias de cámaras
4. Áreas
5. Áreas de intrusión
6. Zonas de intrusión
7. Cámaras de reconocimiento de placas de matrícula
8. Entradas digitales
9. Salidas digitales
10. Intercomunicador
11. Alarmas
12. Macros
13. Patrollers de Patrullas Policiales

H. Los DGM deberán proporcionar la habilidad de dibujar y mostrar información sobre el mapa en la siguiente forma:

   1. Formas vectoriales: líneas, rectángulos, polígonos y elipses
   2. Fotos
   3. Texto

I. Los DGM deberán proporcionar la habilidad de visualizar cualquier tipo de entidades de terceros integradas mediante un SDK. *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

J. Los DGM deberán proporcionar la habilidad de mostrar capas de información en el formato Keyhole Markup Language (KML).

K. El DGM deberá proporcionar la habilidad al operador de administrar capas de entidades visualizadas sobre el mapa, y ser capaz de encenderlas y apagarlas y cambiar el orden de superposición.

L. El DGM proporcionará la capacidad para importar capas de datos de uno o más servidores ESRI ArcGIS.

M. La DGM proporcionará a los operadores la capacidad para gestionar capas que son importadas de ESRI ArcGIS. Los usuarios podrán habilitar y deshabilitar las capas, al igual que clasificarlas.

N. Los DGM deberán ofrecer una copia de seguridad y restauración de datos de mapa integrada tanto para los fondos del mapa como para las capas de entidades.

O. El DGM proporcionará la capacidad de importar configuraciones desde un archivo externo como:

   1. Capa de AutoCAD para objetos
   2. CSV, archivo de Excel

P. Los DGM deberán ofrecer capacidades de conmutación por error.

Q. Los DGM deberán ampliarse a varias miles de entidades sobre un solo mapa y cientos de mapas.

R. Los DGM deberán proporcionar un medio para actualizar el fondo de un mapa sin afectar la configuración del objeto de mapa.

S. Los DGM deberán ofrecer un diseñador de mapas gráficos fácil de usar para configurar los mapas.

T. Los DGM deberán proporcionar una navegación fácil e intuitiva que incluya:

   1. La habilidad para crear jerarquías de mapas para facilitar la navegación dentro y entre varios sitios y edificios.
   2. La habilidad para definir favoritos para una recuperación de posición recurrente.

3. La posibilidad de crear vínculos entre mapas. Los enlaces de los mapas deberán permitir el vínculo desde un mapa a múltiples mapas que representan los pisos de un edificio. Mantener el nivel del mapa cuando se navegue por los pisos de un edificio

4. Una experiencia común de usuario en relación a la navegación en el mapa para GIS y para mapas privados. *(Especificador, se requiere Plan Manager Advanced para GIS)*

U. Deberá ser posible monitorear el estado de entidades en el mapa. Deberá ser posible personalizar los íconos de cualquier entidad representada en el mapa.

V. Los DGM deberán ofrecer la habilidad de establecer de forma opcional una notificación de visualización gráfica de la detección de movimiento.

W. Los DGM deberán ofrecer una herramienta inteligente de selección para tener acceso al video. Al hacer clic en la ubicación que el usuario quiere ver, el DGM seleccionará de forma automática las cámaras que pueden ver esta ubicación y mover el PTZ hacia dicha ubicación. Esta herramienta inteligente de selección deberá tomar los obstáculos en consideración y no mostrar las cámaras que no pueden ver la ubicación debido a una pared.

X. Deberá ser posible seleccionar una ubicación dibujando una zona de interés en el DGM, y para visualizar todas las entidades que forman parte de dicha zona de interés a la vez.

Y. El usuario deberá ser capaz de seleccionar y visualizar el contenido de múltiples entidades de la USP sobre el mapa en las ventanas emergentes.

Z. El usuario deberá ser capaz de mover, redimensionar y fijar las ventanas emergentes de la entidad USP sobre el mapa.

AA. Deberá ser posible tener acceso a video en vivo y en modo de reproducción desde el mapa.

BB. Deberá ser posible monitorear desde el DGM todas las notificaciones de evento de entidades. Los usuarios podrán encender y apagar las notificaciones por entidad.

CC. Los DGM deberán ofrecer la habilidad de operar completamente la supervisión de alarma. Deberá ser posible:

1. Centrar el mapa sobre entidades relacionadas con la alarma.

2. Visualizar las notificaciones de alarma sobre el mapa y tener acceso a los videos relacionados del mapa.

3. Activar y recibir alarmas.

4. Actuar sobre la alarma desde los DGM, incluyendo reconocimientos, reenvíos e investigación.

5. Visualizar que una alarma ocurrió en un mapa vinculado subyacente.

DD. Los DGM deberán proporcionar las siguientes capacidades de búsqueda:

1. Buscar y centrar por nombre de entidad.
2. Desde la Visualización de una entidad en la USP, ubique la entidad en el mapa y ofrezca la posibilidad de seleccionar otra cercana.
3. Por dirección postal, ciudad, punto de referencia, punto de interés (con licencia de geocodificador de Google, ESRI u otro proveedor).

EE. Cualquier actualización del contenido del mapa por parte de un administrador se enviará de forma inmediata y dinámica a todos los usuarios de DGM.

FF. El DGM deberá soportar el uso de mapas GIS o mapas privados o una combinación de ambos para el fondo del mapa. *(Especificador, se requiere Plan Manager Advanced para GIS)*

GG. El DGM deberá ser compatible con cualquier mapa compatible con GIS con el OGC y con WMTS y WMS de soporte. Esto incluye, más no se limita a, mapas ESRI. El DGM deberá permitir la selección de las capas GIS adecuadas. *(Especificador, se requiere Plan Manager Advanced para GIS)*

HH. Los DGM deberán proporcionar un diseñador de mapas intuitivo para el posicionamiento de la entidad sobre el mapa usando la opción arrastrar y colocar. Cualquier configuración deberá ser gráfica.

II. Será posible editar y configurar múltiples objetos del mapa a la vez.

JJ. Todas las modificaciones en el diseño del mapa se conectarán a un registro de auditoría.

KK. Estarán disponibles varias acciones dentro de los mapas para que se ejecuten con un doble clic simple e intuitivo, con un clic en el botón derecho o la funcionalidad de arrastrar y soltar. Los ejemplos de acciones disponibles a través de los mapas deberán incluir el desbloqueo de puertas y el reconocimiento de una alarma.

LL. Mediante la siguiente funcionalidad, los DGM deberán permitir la administración de alarmas de la USP desde el mapa: *(Especificador: se requiere licencia adicional para Plan Manager Standard y versiones superiores)*

1. Ubicar sobre el mapa entidades relacionadas con la alarma.
2. Mostrar entidades de la alarma con un icono específico, color, nivel de transparencia y velocidad de intermitencia.
3. Listar, seleccionar y ubicar alarmas.
4. Centrado automático del mapa sobre la alarma con mayor prioridad.
5. Manejar la alarma desde el mapa, incluyendo reconocimientos, reenvíos e investigaciones
6. Todos los contenedores del mapa, como puntos activos o enlaces del mapa deberán reflejar el estado de la alarma de las entidades contenidas.

MM. Deberá ser posible agregar funcionalidad avanzada al objeto del mapa usando el SDK. Cualquier funcionalidad disponible mediante el SDK de la USP estará disponible dentro de los mapas. *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

NN. Los DGM deberán ofrecer la herramienta de lazo para:

1. Mostrar entidades en un sitio a través de una sola acción.
2. Activar una acción en todas las entidades de un sitio con un solo clic.
3. Editar múltiples entidades de un solo sitio en forma simultánea.

OO. Los DGM deberán permitir la visualización de las entidades de la USP seleccionadas desde el mapa sobre un monitor remoto (pared de video). *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

PP. El DGM deberá permitir realizar búsquedas en el mapa por nombre de la entidad.

QQ. Los DGM deberán permitir el uso de la información KML de mapas superpuestos tanto para mapas GIS como privados. Los objetos movibles deberán estar soportados mediante el uso de KML. *(Especificador, solo Plan Manager Advanced, se requiere licencia adicional)*

RR. El Contratista deberá proporcionar licencias para cada entidad que requiere ser mostrada en los mapas gráficos. *(Especificador, las licencias se venden en paquetes con base en la cantidad de entidades, especificar la licencia de un sitio o ilimitado después de 1,000 entidades)*

2.40 Auditoría y Registros de Actividades de Usuario de la USP (Registros)

A. La USP deberá soportar la generación de registros de auditoría. Los registros de auditoría deberán consistir de registros de adiciones, eliminaciones y modificaciones del operador/administrador,

B. Los registros de auditoría deberán generarse como informes. Deberán contar con la capacidad de rastrear cambios dentro de períodos de tiempo específicos. También deberá ser posible la consulta sobre usuarios específicos, cambios, entidades afectadas y períodos de tiempo.

C. Para los cambios de configuración de entidades, el informe de registros de auditoría deberá incluir información detallada sobre el valor antes y después de los cambios.

D. La USP deberá soportar la generación de registros de actividad del usuario. Los registros de actividad del usuario deberán consistir de registros de la actividad del operador en la USP como inicio de sesión, cámaras vistas, eventos ALPR, impresión de tarjetas de identificación, exportaciones de videos y otros.

E. El ACS deberá soportar las siguientes acciones sobre un informe de registros de auditoría y actividad: impresión y exportación de informes a un archivo PDF/Microsoft Excel/CSV.

2.41 Informes de Incidentes de la USP

A. Los informes de incidentes deberán permitir al operador de seguridad crear informes sobre incidentes que se presentaron durante un turno. Serán soportados los informes de incidentes relacionados con video y los incidentes relacionados con el control de acceso.

B. El operador será capaz de crear informes de incidentes independientes o informes de incidentes enlazados con las alarmas.

C. El operador deberá ser capaz de vincular secuencias múltiples de video a un incidente, tener acceso a los mismos, y cambiar la fecha u hora de las secuencias posteriormente.

D. Deberá ser posible crear una lista de categorías de Incidentes, etiquetar una categoría a un incidente, y filtrar la búsqueda con la categoría como parámetro.

E. Los informes de incidentes deberán permitir la creación de un formulario personalizado sobre el cual se incluya la información sobre un incidente.

F. Los informes de incidentes deberán permitir agregar entidades, eventos y alarmas para soportar las conclusiones del informe.

G. Los informes de incidentes permitirán el uso de un logotipo personalizado, el logotipo predeterminado de Mission Control o ningún logotipo.

2.42 Ingestión de datos de USP

A. La USP deberá permitir la posibilidad de importar datos externos de fuentes externas para mejorar la unificación de las fuentes de datos dentro de la USP.

B. Cada fuente de datos se definirá mediante un conjunto de campos y tipos de campo que describen la fuente de datos. Los tipos de campo serán:

1. Cadena
2. Entero de 32 bits y 64 bits
3. Número de coma flotante
4. Booleano
5. Marca de tiempo
6. Binario (en un archivo o base 64)

C. La visualización de cada punto de datos de una fuente de datos será configurable para determinar qué campos de los datos deben mostrarse. La configuración de cada campo debe ser:

1. Qué campos se muestran u ocultan
2. En qué orden se muestran los campos

3. Una etiqueta para especificar el nombre del campo (en formato clave:valor)
4. Una opción para especificar cómo mostrar el campo (valor de texto, imagen, valor del portapapeles, hipervínculo a una página web, hipervínculo a una entidad en el sistema, archivo de sonido)

D. Debe haber un privilegio disponible para cada fuente de datos para permitir o denegar el acceso a usuarios específicos y grupos de usuarios de la USP.

E. Los datos ingeridos estarán disponibles en el sistema de informes de la USP.

F. Los datos ingeridos estarán disponibles para mostrarse en los tableros de control de la USP.

2.43 Integración de terceros de USP

A. Integración de Microsoft Active Directory: *(Especificador, Professional y versiones superiores, se requiere licencia adicional)*

1. La USP deberá soportar una conexión directa a uno o varios servidores de Microsoft Active Directory mediante la(s) Función(es) del Active Directory. La integración del Active Directory deberá permitir la sincronización de información desde el servidor del Active Directory a la USP.
2. La integración del Active Directory deberá permitir la administración central de los usuarios, grupos de usuarios, tarjetahabientes y grupos de tarjetahabientes de la USP.
3. La USP deberá soportar ADFS para el inicio de sesión de los usuarios.
4. La USP deberá ser capaz de conectarse y sincronizar datos desde múltiples servidores de Active Directory (hasta 10).
5. La USP deberá soportar Active Directory de Azure para la sincronización de los tarjetahabientes.
6. La USP deberá soportar la sincronización de Grupos Universales del Active Directory al igual que la de grupos de seguridad que pertenecen a otros dominios dentro del mismo bosque.
7. La USP deberá soportar la encriptación del Microsoft Active Directory usando LDAP SSL.
8. Al estar habilitado, el Active Directory deberá administrar el inicio de sesión del usuario a las aplicaciones de la USP del cliente a través de las credenciales Windows del usuario. El inicio de sesión a la USP deberá utilizar características de administración y autenticación de contraseñas nativas del Active Directory.
9. Deberá ser posible sincronizar las siguientes entidades de la USP y su información desde el Active Directory con la USP:
    a. Usuarios (nombre de usuario, nombre y apellido, dirección de correo electrónico y demás)

b. Grupos de usuarios (nombre del grupo de usuarios, descripción y dirección del correo electrónico del grupo)

c. Tarjetahabientes (nombre y apellido, descripción, correo electrónico, foto y otros)

d. Grupos de tarjetahabientes (nombre del grupo de tarjetahabientes, descripción y dirección de correo electrónico del grupo)

e. Atributos del Active Directory a los campos personalizados de la USP

10. Al estar habilitado, la adición, eliminación o suspensión de la cuenta Windows del usuario en el Active Directory deberá resultar en la creación, eliminación o deshabilitación de la cuenta de usuario equivalente en la USP.

11. Cuando está habilitado, la adición, eliminación o suspensión de la cuenta Windows del usuario en el Active Directory deberá resultar en la creación, eliminación o deshabilitación de la cuenta del tarjetahabiente equivalente en la USP.

12. Los métodos de sincronización admitidos para adiciones, modificaciones y eliminaciones de entidades sincronizadas deberán incluir en el primer inicio de sesión (solo usuarios), sincronización manual y sincronización programada.

13. La USP deberá soportar las conexiones de los usuarios a través de organizaciones independientes al conectarse a un proveedor de identidad externo mediante una autenticación basada en notificaciones, como ADFS (Active Directory Federation Services), Azure Active Directory, otros proveedores de OpenID Connect y SAML2.

B. Integración de Detección de Intrusión: *(Especificador, Standard, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte el documento de Plugins Compatibles con Security Center)*

1. La USP se deberá integrar con los paneles de intrusión y dispositivos de terceros mediante un SDK de Intrusión. La Función del Intrusion Manager deberá manejar las comunicaciones con los paneles de intrusión. Las comunicaciones con los dispositivos de intrusión deberán ser sobre comunicaciones en serie y/o una red IP.

2. Deberá ser posible la integración con los paneles de intrusión fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.

3. La funcionalidad disponible mediante la integración de dispositivos de intrusión con la USP deberá incluir lo siguiente (en donde sea soportado por el panel de intrusión):

a. Activar y desactivar dispositivos de intrusión (de forma manual, en un horario determinado o después de un evento de la USP)

b. Activar o accionar salidas de dispositivos de intrusión

c. Ver eventos y alarmas de intrusión

d. Supervisar el estado, incluyendo el estado de activación, de los dispositivos de intrusión

e. Verificar por video los eventos y las alarmas de intrusión con paneles de video

f. Crear zonas de la USP con entradas de dispositivos de intrusión

4. Los paneles de intrusión actualmente soportados incluyen:

a. Paneles Bosch de la serie G

b. Bosch Map 5000

c. Paneles DSC de la serie Power

d. Paneles DMP de la serie XR

e. Paneles Honeywell Galaxy Dimension y Flex

f. Vanderbilt SPC

g. UTC Advisor Master y Advanced

5. Los siguientes son algunos de los dispositivos de intrusión adicionales compatibles:

a. BuyTime

b. Receptor de panel de alarmas

c. Southwest Microwave RPMII

C. Sistemas de Control de Acceso de Terceros: *(Especificador, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte la guía de Plugins compatibles con Security Center)*

1. La USP deberá integrarse con software de control de acceso de terceros a través del SDK. Las comunicaciones con software de control de acceso se producirán a través de una red IP y no deberían soportar tareas administrativas como la administración de tarjetahabientes.

2. Deberá ser posible la integración con software de control de acceso fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.

3. La funcionalidad disponible mediante la integración de software de control de acceso con la USP deberá incluir lo siguiente (en donde sea soportado por la solución de control de acceso):

a. Sincronice entidades de control de acceso y reciba estados y eventos asociados dentro de la USP, lo que incluye:

i. Derechos de acceso y tarjetahabientes

ii. Visitantes

iii. Lectores y puertas

iv. Alarmas

v. Entradas y salidas

b. Monitorear eventos de control de acceso

c. Monitorear y reconocer alarmas de control de acceso

d. Activar acciones y salidas en el software de control de acceso usando acciones activas y eventos a toma de acción

e. Bloquear y desbloquear puertas en el software de control de acceso

f. Verificación por video de eventos y alarmas de control de acceso

g. Configurar eventos a toma de acción usando los eventos y las alarmas de control de acceso

h. Generar informes de Security Center mediante el uso de datos de control de acceso

i. Visualizar y monitorear estados de entidades de puertas en los mapas de la USP

4. Entre los fabricantes de control de acceso actualmente compatibles, se encuentran los siguientes:

a. Tyco Software CCURE

b. UTC Lenel Onguard

c. Amag Symmetry

d. Siemens Sipass

e. AssaAbloy ARX

D. Sistemas de Distribución de Destinos de Terceros: *(Especificador, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte la guía de Plugins compatibles con Security Center)*

1. La USP deberá integrarse con software de distribución de destinos (control de elevadores) de terceros a través del SDK. Las comunicaciones con el software de distribución de destinos se deberán realizar en una red IP.

2. Deberá ser posible la integración con software de distribución de destinos fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.

3. La funcionalidad disponible mediante la integración de software de distribución de destinos con la USP deberá incluir lo siguiente (en donde sea soportado por la solución de distribución de destinos):

a. Creación de entidades de la distribución de destinos y recepción de eventos y estados relacionados dentro de la USP, incluyendo lo siguiente:

i. Pisos y descansos

ii. Carros de elevadores (puertas delanteras y traseras) y quioscos

iii. Tarjetahabientes y credenciales (si corresponde)

b. Monitoreo de eventos de distribución de destinos.

c. Activación de acciones manuales de distribución.

d. Verificación por video de eventos de distribución de destinos.

e. Configuración de eventos a toma de acción mediante eventos de distribución de destinos.

f. Generación de informes de Security Center con los datos de la distribución de destinos.

g. Compatibilidad con varios lectores:

i. Lectores internos de quioscos

ii. Lectores de la USP

h. Tipos de pasajeros y modos avanzados de quioscos.

4. Entre los fabricantes de distribución de destinos actualmente compatibles, se incluyen los siguientes:

a. Otis Compass

b. Thyssenkrupp

c. Schindler

d. MCE

E. Integración de Administración de Activos: *(Especificador, se requiere licencia adicional, Professional y versiones superiores)*

1. La USP se deberá integrar con los sistemas de administración de activos de terceros mediante la Función de Administración de Activos.

2. Las comunicaciones con las soluciones de la administración de activos deberán ser sobre una red IP (mediante comunicaciones de software).

3. La funcionalidad disponible mediante la integración de sistemas de administración de activos con la USP deberá incluir lo siguiente (en donde lo soporten los sistemas de administración de activos):

a. Sincronización de los activos del sistema de administración de activos con las entidades de activos de la USP.

b. Monitoreo en vivo de los eventos de actividades relacionadas con activos, eventos de los estados de salud y actividad (activo en línea, activo fuera de línea, movimientos de activo o baja batería).

c. Sincronización de alarmas de administración de activos con las alarmas del Security Center.

d. Visualización de video enlazado a actividades y alertas relacionadas con activos dentro de las tareas de generación de informes y monitoreo.

e. Reconocimiento de alarmas en Security Center el cual reconoce alertas en el sistema de administración de activos y viceversa.

f. Seguimiento en tiempo real de ubicaciones de activos por áreas.

g. Tarea de generación de informes de Inventario de Administración de Activos que muestra a detalle la ubicación actual (área) de un activo.

h. Tarea de generación de informes de Actividad de Activos que proporciona un resumen histórico de eventos y actividades relacionadas con activos.

4. Los sistemas de administración de activos actualmente compatibles incluyen:

a. Administración de claves Deister

b. Morsewatchmans

c. TRAKA

F. Integraciones Adicionales de Terceros

1. La USP deberá soportar enfoques múltiples para la integración de sistemas de terceros. Estas deberán incluir: Kits de Desarrollo de Software (SDK), SDK de Servicio de Web basado en REST, SDK de Servicio RTSP, entre otros. *(Especificador, Professional y versiones superiores, se requiere licencia y paquete SDK)*

2. La arquitectura de la USP deberá soportar la adición de nuevas conexiones para adaptarse a la integración de sistemas de terceros, por ejemplo: *(Especificador, consulte el sitio web para ver cómo se otorgan las licencias; para obtener una lista actualizada de las Integraciones de Terceros, consulte la guía de plugins compatibles)*

a. Sistemas de video de terceros

b. Sistemas de control de acceso de terceros

c. Integraciones de ALPR con estaciones de pago, proveedores de permisos, proveedores de pagos por teléfono y vendedores de boletos

d. Sistemas de administración de edificios

e. Ecosistema de Control de Acceso (como ID Scanner, sincronización de tarjetas, Guardtour y Morpho Biometrics)

f. Monitoreo de transacciones (POS, escaneo de códigos de barras y cajeros automáticos)

g. IoT Industrial (Modbus, BACnet, OPC, SNMP)

h. Industrial Protocol Interface (BACnet, Modbus)

i. Pared de video (Barco, Eizo)

j. Sistemas de administración de recursos humanos (HRMS)

k. Integración de Drones Autónomos

l. Teclas Inteligentes (Salto SVN, Medeco XT, CLIQ)

m. Detección de Disparos (Shot Spotter, Guardian GunShot)

n. Libro de Registro Dinámico

o. Plataforma de Reconocimiento Facial

p. Servicios de Localización en tiempo real - RTLS (HID)

2.44 Kit de Desarrollo del Software (SDK, por sus siglas en inglés) de la USP *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

A. Un SDK de la USP deberá estar disponible para soportar el desarrollo personalizado para la plataforma.

B. El SDK deberá incluir funcionalidades específicas de los sistemas embebidos de reconocimiento automático de placas de matrícula (ALPR), control de acceso (ACS) y videos (VMS).

C. La integración con aplicaciones y bases de datos externas deberá ser posible con el SDK.

D. El SDK deberá soportar una API para permitir la integración de hardware de control de acceso de terceros.

E. El SDK deberá permitir a los usuarios finales desarrollar nuevas funcionalidades (interfaz de usuario, aplicaciones independientes o servicios) para enlazar la USP a sistemas y aplicaciones administrativos de terceros como Sistemas para Uso de Emblemas, Sistemas de Administración de Recursos Humanos (HRMS), y Sistemas de Planificación de Recursos Empresariales (ERP).

F. El SDK deberá basarse en la plataforma .NET.

G. El SDK deberá soportar actualizaciones dinámicas y transaccionales a la configuración de la USP. También deberá soportar el cambio de notificación de la configuración de entidad de la USP.

H. El SDK deberá proporcionar una lista completa de las funciones de programación para ver y/o configurar entidades básicas como lo son: usuarios y grupos de usuarios, alarmas, eventos personalizados, cronogramas. etc.

I. El SDK deberá proporcionar una lista completa de funciones de programación para ver y configurar el ACS, el VMS y el ALPR.

J. El SDK deberá proporcionar una lista completa de funciones de programación para ver y configurar la mayoría de las entidades de ACS, como tarjetahabientes, grupos de tarjetahabientes, visitantes, credenciales, reglas de acceso (solo modificaciones) y campos personalizados.

K. El SDK deberá ser capaz de recibir eventos en tiempo real desde las siguientes entidades de la USP: usuarios y grupos de usuarios, áreas, zonas, cámaras, unidades de videos, puertas, controladores de puerta (unidades), elevadores, tarjetahabientes, grupos de tarjetahabientes y credenciales.

L. El SDK deberá ser capaz de consultar el historial de eventos para áreas, cámaras, zonas, alarmas, tarjetahabientes, credenciales, visitantes, puertas, eventos de lectura de consultas de placa de matrícula, eventos de aciertos de placas de matrícula automotriz, generar un informe de aciertos de placa de matrícula , generar un informe de lecturas de placa de matrícula.

M. El SDK deberá soportar las siguientes funciones de alarma: visualización de alarmas en tiempo real, reconocimiento de alarmas, cambiar prioridades y cambiar destinatario.

Parte 3 - Ejecución

3.01 Garantía

A. El producto deberá desarrollarse en todos los aspectos materiales de acuerdo con el manual del usuario adjunto, y los medios en donde resida el Software del Producto estarán libre de defectos en material y mano de obra bajo uso normal. Los defectos de software están cubiertos mediante Lanzamiento de Servicios y Actualizaciones Acumulativas las cuales están disponibles por un 1 año a partir de la fecha de la compra del software.

B. La garantía prolongada, hasta por 5 años, deberá estar disponible mediante la compra del servicio de asistencia de Genetec, el cual incluye los siguientes servicios adicionales además de la garantía estándar:

1. Acceso a soporte telefónico y chat en línea para asistencia técnica.
2. Administración de caso en línea
3. System Availability Monitor en línea
4. Acceso a Actualizaciones de Versiones Importantes y Secundarias
5. Soporte de localizador 24/7 y especialistas dedicados de soporte *(Prescriptor, costo adicional)*

3.02 Puesta en marcha del sistema y servicios de integración *(Especificador, este es un cobro diario más viáticos, revisar Genetec Inc. para ver el número recomendado de días a especificar)*

A. Requisitos Generales:

1. El contratista deberá ocupar los servicios del integrador de la USP para asistir en la administración de la integración de la USP en el sitio del usuario final en proyectos que involucren:
    a. Varios contratistas o subcontratistas serán responsables por la integración de la USP en varios sitios del cliente en diferentes zonas geográficas.
    b. Las instalaciones empresariales complejas que involucran funcionalidades avanzadas (como la característica de Federation™, conmutaciones por error y plugins), sistemas múltiples (como control de acceso, videos y ALPR) o integraciones de terceros.
    c. El amplio uso de soluciones/plugins personalizados desarrollados por el integrador que se integrarán en la USP.
2. Los servicios del integrador de la USP deberán incluir la Administración de la Integración y Configuración y Puesta en Marcha del Sistema.

B. Servicio de Administración de Implementación:

1. El servicio de Administración de Integración del integrador deberá incluir un Gerente de Proyecto que actúa como el único punto de contacto para todas las comunicaciones entre el contratista y la organización del proveedor quién será el responsable de:
    a. Llevar a cabo la Evaluación de Riesgo del impacto sobre posibles factores de riesgo en el funcionamiento de la USP del integrador.
    b. Proporcionar un plan de proyecto para la integración de la USP del integrador.
    c. Administrar el desarrollo e implementación de los componentes de la solución personalizada que se integrarán a la USP del proveedor (si corresponde).
    d. Proporcionar un ámbito del trabajo que indique en detalle los servicios ofrecidos por el proveedor para asistir en la implementación de la USP del integrador.
    e. Coordinar y programar los servicios en campo del proveedor con el contratista para asistir en la implementación de la USP del proveedor.
    f. Proporcionar actualizaciones regulares del estado del proyecto al contratista en relación a la implementación de las soluciones personalizadas (si corresponde) y la implementación de la USP del proveedor.

C. Servicio de Arquitecto de Soluciones:

1. El servicio de Arquitecto de Soluciones del proveedor deberá incluir un ingeniero de arquitectura de soluciones que actúe como único punto de contacto técnico durante la implementación de la USP y que será responsable de lo siguiente:
    a. Asistir al contratista/subcontratista con el diseño y la arquitectura de la USP del proveedor.

b. Llevar a cabo actividades de consulta técnica que podrían incluir análisis de deficiencias/ajustes, revisiones de diseño del sistema, evaluaciones de compatibilidad de dispositivos, revisiones de diseño funcional y técnico, así como revisiones de rendimiento de la USP del proveedor.

c. Realizar una evaluación del sistema y garantizar el cumplimiento de las mejores prácticas de la USP del proveedor.

d. Proporcionar una estrategia de migración y actualización para la USP del proveedor según corresponda.

e. Proporcionar documentación con relación a la arquitectura del sistema, el diseño del sistema, las especificaciones de hardware y los requisitos de compatibilidad, los cálculos del ancho de banda de las cámaras y las mejores prácticas con respecto a la USP del proveedor.

D. Servicio de Configuración y Puesta en Marcha de Sistemas:

1. La Configuración del Sistema y el Servicio de Puerta en Marcha del proveedor deberá incluir un Ingeniero de Campo quien será responsable por:

a. Asistir a los técnicos en el lugar/remotos del contratista o subcontratista con la configuración y puesta en marcha de la USP del proveedor en el sitio del cliente.

b. Llevar a cabo una prueba de la USP después de la instalación del sistema usando escenarios del operador reales para asegurar un desempeño óptimo del sistema.

c. Proporcionar al contratista con un Informe de Servicio que indique con detalle las tareas realizadas durante la integración de la USP en el sitio del cliente, al igual que recomendaciones para mejorar el desempeño de la USP que deben ser implementadas por el contratista.

d. Proporcionar una transferencia de conocimiento de la USP del proveedor al contratista después de la implementación de la USP en el sitio del cliente.

3.03 Capacitación del Fabricante para el Operador Usuario Final *(Especificador: Este es un cargo de medio día más gastos)*

A. El contratista deberá contratar los servicios del proveedor de la USP para asistir en la capacitación del usuario final de la USP en el sitio final del usuario.

Fin de la Sección

Sección 28 17 00 Sistema de Administración de Acceso e Identidad Física

Parte 1 - Información General

1.01 Trabajo relacionado

A. Sección 28 13 00 – Software de Control de Acceso y Administración de Base de Datos

1.02 Definiciones

A. ACS - Sistema de Control de Acceso

B. CSA - Aplicación de Software del Cliente

C. DGM - Mapas Gráficos Dinámicos

D. ALPR – Reconocimiento Automático de Placas de Matrícula

E. SDK - Kit de Desarrollo de Software

F. GLM – Administración del Ciclo de Vida de Genetec

G. SSM - Módulo de Software del Servidor

H. UI - Interfaz de Usuario

I. USP - Plataforma Unificada de Seguridad

J. USW - Cliente Web Unificado

K. VMS - Sistema de Administración de Videos

L. PIAM – Administración de Acceso e Identidad Física

M. SLA – Acuerdo de Nivel de Servicio

N. API – Interfaz de Programación de Aplicaciones

O. HSM – Módulo de Seguridad de Hardware

P. FIPS – Estándares Federales para el Procesamiento de Información

Q. HTTPS – Protocolo Seguro de Transferencia de Hipertexto

R. TLS – Transport Layer Security

S. AES – Estándar de Encriptación Avanzada

T. SSO – Inicio de Sesión Única

U. AD – Active Directory

1.03 Requisitos

A. El programador del sistema deberá haber asistido a la capacitación del fabricante, junto con las siguientes certificaciones:

1. Certificación Técnica de Security Center 5.x Synergis™ (SC-STC-001)
2. Configuración Avanzada y Solución de Problemas de Security Center 5.x Synergis™ (SC-STC-002)
3. Security Center 5.x ClearID – Nivel 2 (SC-CID-002)

B. El programador del sistema deberá tener el estado de nivel “Acreditado” en el Programa de Socios de Canal de Genetec con el siguiente nivel de calificación: *(Especificador, seleccione uno de los siguientes)*

1. Socio de Negocios Certificado o superior
2. Socio de Negocios Élite o superior
3. Socio de Negocios Élite Unificado

C. El programador del sistema deberá presentar comprobante de las certificaciones.

Parte 2 - Productos

2.01 Sistema de Administración de Acceso e Identidad Física (PIAM, por sus siglas en inglés)

A. El PIAM será un Sistema de Administración de Acceso e Identidad Física de clase empresarial. Deberá integrarse por completo dentro de una Plataforma de Seguridad Unificada (USP, por sus siglas en inglés). La USP deberá permitir la integración fluida del PIAM con un Sistema de Control de Acceso (ACS, por sus siglas en inglés).

B. El sistema PIAM deberá ser altamente escalable para implementaciones globales.

1. El sistema PIAM deberá admitir configuraciones con múltiples sistemas de Control de Acceso.
2. El sistema PIAM deberá admitir la concesión de licencias hasta:
    a. 1 000 000 de identidades únicas
    b. 500 sitios
    c. 1000 quioscos para visitantes
    d. 1 000 000 visitas anuales
3. Además, cada cuenta admitirá hasta:
    a. 10 000 funciones, con hasta 100 000 identidades en una función
    b. 200 000 áreas

E. El sistema PIAM deberá admitir diversas funcionalidades de administración de identidad, que incluyen, entre otras:

1. Administración programable de tarjetahabientes para asignación automática de acceso
2. Administración manual de tarjetahabientes mediante flujos de trabajo

F. Fabricante:

1. Genetec ClearID

G. Certificación:

1. El sistema PIAM deberá ser un Sistema de Administración de Seguridad de la Información con certificación ISO/IEC 27001:2013.

2.02 Arquitectura

A. Arquitectura de nube distribuida globalmente:

1. Microsoft Azure
   a. Servicios globales distribuidos
      i. Políticas y reglas
      ii. Autenticación de usuarios
      iii. Administración de áreas
      iv. API
      v. Portal de autoservicio
      vi. Motor de flujos de trabajo
      vii. Notificación de correo electrónico
      viii. Aprovisionamiento automático
   b. Servicios Regionales
      i. Las identidades y las credenciales de tarjetahabientes se almacenan en el centro de datos de Azure más cercano al usuario.
      ii. Los datos se distribuyen en repositorios independientes en silos.
   c. Sitios locales
      i. Security Center Synergis™
      ii. Campos personalizados locales
      iii. plugins
2. Alta disponibilidad
   a. 99,9% SLA
   b. Almacenamiento de datos con redundancia geográfica

3. Controles de Seguridad
    a. Encriptación de datos
        i. AES 256
        ii. RSA 2048
        iii. Claves simétricas y claves asimétricas
            a. Las claves se administran mediante Azure Key Vault
                i. HSM validados según FIPS 140-2 de nivel 2
    b. Integridad de los datos
        i. Las firmas digitales basadas en SHA 512 con RSA 2048 se usan para validar los datos.
    c. Encriptación de comunicaciones
        i. Protocolo Seguro de Transferencia de Hipertexto (HTTPS) TLS 1.2
        ii. Certificados de Transport Layer Security (TLS)
    d. Arquitectura de confianza cero
        i. Los datos del cliente se segmentan en microservicios, que solo tienen el acceso mínimo a los datos que se requiere para realizar esa tarea.
            a. Toda la comunicación entre microservicios se encripta y firma de manera digital.
    e. Monitoreo de servicios
        i. Los controles se actualizan en función de diversos servicios y fuentes de amenazas de seguridad.
        ii. El sistema ejecuta análisis de métricas constantes, incluidas transacciones sintéticas para emular la actividad de usuarios.
        iii. Los equipos de desarrollo y operaciones monitorean los sistemas y se les notifica de cualquier problema.
    f. Autenticaciones de usuarios
        i. Azure Active Directory (AD) B2B de forma predeterminada
        ii. Opción de federación de identidades de usuarios de AD existentes a través de Azure AD B2B u OpenID Connect para proporcionar Inicio de Sesión Única (SSO, por sus siglas en inglés).
            a. También admite:
                i. OneLogin
                ii. Okta
                iii. Auth0
                iv. Ping
                v. MyID

B. Plugin de Clear ID

1. Instalado en un servidor de Security Center para integrar Genetec ClearID y Security Center, proporcionando comunicaciones entre Synergis™ y los Servicios en la Nube de ClearID.
2. El plugin también se instala en una estación de trabajo de la Config Tool, lo que le permite al administrador crear y configurar la función del plugin, y configurar los ajustes de la base de datos y los ajustes de conexión para ClearID.
3. El complemento se actualizará de forma automática si hay una conexión a Internet disponible cuando Genetec publique una nueva versión.

2.03 administración

A. Gestión de identidades

1. Información de identidad:
   a. Información personal general
   b. Información de la empresa
   c. Supervisores de esta identidad
   d. El sistema sincronizará la información de identidad con las siguientes fuentes:
      i. Archivo CSV exportado desde una base de datos de RR. HH.
      ii. Base de datos de Microsoft SQL Server u Oracle
      iii. Microsoft Active Directory a través del LDAP
   e. El sistema deberá tener una API REST de Identidad disponible de forma externa para la sincronización de la información de identidad de fuentes externas
2. Control de Acceso
   a. Período de acceso
      i. Fecha de activación
      ii. Fecha de vencimiento
   b. Atributos de aprovisionamiento
   c. Tarjetahabientes asociados
3. Permisos de Usuario
   a. El administrador puede habilitar o deshabilitar el acceso de los usuarios al portal web
   b. El administrador puede asignar tipos de usuarios:
      i. Administrador
      ii. Usuario

4. Administración de visitantes
    a. El administrador puede otorgar permisos de usuario para invitar visitantes a sitios específicos

B. Administración de Áreas

1. Administración de Áreas
    a. Los propietarios y aprobadores de áreas pueden ver, agregar y quitar funciones de las áreas.
    b. Los administradores pueden asignar la administración a uno o más propietarios de áreas.
    c. Los propietarios y aprobadores de áreas pueden delegar sus tareas a otra persona de la organización mientras están de licencia (por ejemplo, vacaciones, enfermedad y demás). El delegado tendrá el mismo conjunto de permisos que el delegador y podrá administrar las tareas en su nombre.
2. Control de Acceso
    a. Los propietarios y aprobadores de áreas pueden ver, agregar y quitar personas de las áreas.
    b. Los propietarios y aprobadores de áreas pueden otorgar acceso temporal a las funciones.
    c. Se puede solicitar al supervisor del empleado que apruebe la solicitud de acceso del empleado.
    d. Los aprobadores pueden procesar las solicitudes de acceso mediante el portal web de ClearID.
    e. Los supervisores de empleados pueden delegar sus tareas a otra persona de la organización mientras están de licencia. El delegado tendrá el mismo conjunto de permisos que el delegador y podrá administrar las tareas en su nombre.
3. Permisos de Usuario
    a. Los propietarios, aprobadores y supervisores de áreas pueden aprobar o denegar las solicitudes de acceso.
    b. Los tarjetahabientes permanentes pueden solicitar acceso temporal a las áreas.
    c. Los tarjetahabientes permanentes pueden invitar visitantes.

C. Administración de funciones

1. Administración de Funciones
    a. Asignar las funciones de administración o el grupo de configuración de tarjetahabientes a uno o más propietarios de funciones.

b. Los administradores de funciones pueden agregar o quitar personas de sus grupos.

c. Los propietarios de funciones pueden asignar acceso a un área para todo su grupo.

d. Aprovisionamiento y sincronización automáticos de grupos de configuración de tarjetahabientes para varios sitios.

e. Los administradores y propietarios de funciones pueden administrar funciones en su dominio utilizando el portal web de ClearID.

f. El propietario y los administradores de funciones pueden delegar sus tareas a otra persona de la organización mientras están de licencia. El delegado tendrá el mismo conjunto de permisos que el delegador y podrá administrar las tareas en su nombre.

2. Aprovisionamiento basado en funciones

a. El acceso se puede otorgar o revocar según las ubicaciones de los empleados.

b. El acceso se puede otorgar o revocar según las funciones o los puestos específicos en la organización, o a quién responden.

c. El acceso se puede otorgar o revocar según la finalización de una capacitación específica o la posesión de los certificados requeridos.

d. El acceso se puede otorgar o revocar según una lista de atributos personalizados sincronizados desde una fuente externa.

e. Se puede configurar un período de gracia para retrasar la revocación del acceso por un período de tiempo configurable después de un cambio en los atributos.

D. Administración de Sitios

1. Administración de Sitios

a. Administración global de tarjetahabientes para múltiples sistemas de Synergis™.

b. Compatibilidad con husos horarios (integrada).

c. Los propietarios del sitio pueden delegar sus tareas a otra persona de la organización mientras están de licencia. El delegado tendrá el mismo conjunto de permisos que el delegador y podrá administrar las tareas en su nombre.

2. Control de Acceso

a. Sincronización automática de credenciales permanentes cuando alguien viaja entre sitios.

b. La sincronización de tarjetahabientes solo sucede cuando se modifican los tarjetahabientes, si el tarjetahabiente tiene acceso en ese sistema de Synergis™.

c. La sincronización de grupos de configuración de tarjetahabientes solo ocurre cuando se modifican los grupos de configuración de tarjetahabientes, si el grupo de configuración de tarjetahabientes tiene acceso a ese sistema de Synergis™.

E. Administración de visitantes

1. Administración de visitantes

a. Importación manual o mediante CSV de prerregistros de visitantes mediante el portal web.

b. El flujo de trabajo de aprobación de visitantes se puede personalizar según el área seleccionada.

c. Las opciones de flujo de trabajo de aprobación de eventos de visita se pueden personalizar al nivel del sitio.

d. Se pueden asignar aprobadores de eventos de visita para aprobar un evento de visita.

e. Los aprobadores de eventos de visita pueden delegar sus tareas a otra persona de la organización mientras están de licencia. El delegado tendrá el mismo conjunto de permisos que el delegador y podrá administrar las tareas en su nombre.

f. Aprovisionamiento automático de visitantes con las áreas requeridas asignadas de manera automática.

g. Registro de visitantes usando Security Desk.

h. El sistema admitirá la configuración de quioscos de autoservicio para el registro de visitantes.

i. El quiosco se basará en hardware de iPad.

ii. Las opciones de quiosco tipo pedestal y de sobremesa pueden estar disponibles.

iii. El quisco admite el prerregistro de visitantes y el registro en el momento.

iv. El quisco admite los idiomas inglés, francés, español, holandés, alemán, italiano y portugués.

v. Los visitantes deberán poder registrarse con una ID gubernamental (más de 200 ID admitidas) o con una dirección de correo electrónico.

a. Consulte la documentación de ClearID para conocer las ID de países admitidas.

vi. Los datos de códigos QR se pueden enviar a los visitantes en un correo electrónico de Confirmación del Visitante antes de la visita. El quiosco deberá tener la capacidad de procesar los datos de códigos QR para el registro de visitantes.

vii. El quiosco deberá tener la capacidad de imprimir una credencial de visitante temporal con credenciales de código QR.

viii. Se puede enviar una alerta por SMS al anfitrión cuando un visitante completa su registro.

ix. El quiosco admite la impresora térmica Brother QL-820NWB.

i. Notificaciones por correo electrónico cuando se crea una solicitud de visita.

j. Notificaciones por correo electrónico cuando se aprueba o deniega una solicitud de visita.

k. Captura e informe del motivo de la visita.

l. Invitación por correo electrónico enviada al visitante con una invitación a la reunión (formato iCalendar - RFC 2445), detalles del sitio y código QR opcional para archivos adjuntos.

m. Notificaciones por SMS y correo electrónico enviados al anfitrión del visitante cuando el visitante se registra.

i. Consulte la documentación de ClearID para conocer los códigos de países admitidos.

2. Control de Acceso

a. Credenciales temporales y distintivos impresos para la administración de visitantes.

b. El código QR de 40 bits que se envía a los visitantes se puede usar como credencial en Security Center.

c. El acceso a áreas específicas se puede restringir por credencial.

d. Se puede exigir un acompañante de visitantes, con hasta 10 anfitriones de visitantes únicos.

e. Los aprobadores pueden procesar las solicitudes de acceso de visitantes mediante el portal web de ClearID.

F. Administración de Plataforma

1. Logotipo corporativo para las notificaciones por correo electrónico y el portal

2. Plataforma en la nube

3. Interfaz web HTML5 con compatibilidad móvil

4. API REST disponible para automatizar cualquier función disponible en el portal web

G. Administración de Autenticación/Seguridad

1. Compatibilidad con autenticaciones de múltiples factores para usuarios que usan OpenID para conectarse

2. Inicio de Sesión Única con Microsoft Office 365

3. Inicio de Sesión Única con Microsoft Azure Active Directory (AD)

4. Certificación ISO 27001:2013

5. Encriptación AES-256 con RSA de 2048 bits
6. El sistema se somete a pruebas de penetración anuales por parte de una empresa de seguridad acreditada externa

Parte 3 - Ejecución

3.01 Ejecución

A. Cumplir con las instrucciones escritas de todos los fabricantes a menos que se indiquen requisitos más estrictos.

3.02 Garantía:

A. El producto deberá desarrollarse en todos los aspectos materiales de acuerdo con el manual del usuario adjunto, y los medios en donde resida el Software del Producto estarán libre de defectos en material y mano de obra bajo uso normal. Con la suscripción de software, los defectos quedan abarcados por la entrega continua de actualizaciones.

B. La suscripción de software incluirá los siguientes servicios de soporte:

1. Soporte telefónico general y chat en línea para asistencia técnica solo durante el horario comercial.
2. Administración de casos en línea a través del GTAP.

3.03 Puesta en marcha del sistema y servicios de integración *(Prescriptor, este es un cobro diario más viáticos, revisar Genetec Inc. para ver el número recomendado de días a especificar)*

A. Requisitos generales:

1. El contratista deberá ocupar los servicios del integrador de la USP para asistir en la administración de la integración de la USP en el sitio del usuario final en proyectos que involucren:
   a. Varios contratistas o subcontratistas serán responsables por la integración de la USP en varios sitios del cliente en diferentes zonas geográficas.
   b. Instalaciones empresariales complejas que involucran funcionalidad avanzada (por ejemplo, las características de Federation, conmutación por error, plugins), sistemas múltiples (por ejemplo, control de acceso, video, ALPR) o integraciones de terceros.
   c. El amplio uso de soluciones/plugins personalizados desarrollados por el integrador que se integrarán en la USP.
2. Los servicios del integrador de la USP deberán incluir la Administración de la Integración y Configuración y Puesta en Marcha del Sistema.

B. Servicio de Administración de Implementación:

1. El servicio de Administración de Implementaciones del proveedor incluirá un Administrador de Proyecto que actuará como el único punto de contacto para

todas las comunicaciones entre el contratista y la organización del proveedor, y que será responsable de lo siguiente:

a. Llevar a cabo una Evaluación de Riesgos del impacto de los posibles factores de riesgo en el funcionamiento de la USP del proveedor.

b. Proporcionar un plan de proyecto para la implementación de la USP del proveedor.

c. Administrar el desarrollo y la implementación de los componentes de la solución personalizada que se integrará a la USP del proveedor (si corresponde).

d. Proporcionar un ámbito del trabajo que indique en detalle los servicios ofrecidos por el proveedor para asistir en la implementación de la USP del integrador.

e. Coordinar y programar los servicios en campo del proveedor con el contratista para asistir en la implementación de la USP del proveedor.

f. Proporcionar actualizaciones periódicas del estado del proyecto al contratista en relación con el desarrollo de soluciones personalizadas (si corresponde) y la implementación de la USP del proveedor.

C. Servicio de Arquitecto de Soluciones:

1. El servicio de Arquitecto de Soluciones del proveedor deberá incluir un ingeniero de arquitectura de soluciones que actúe como único punto de contacto técnico durante la implementación de la USP y que será responsable de lo siguiente:

a. Asistir al contratista/subcontratista con el diseño y la arquitectura de la USP del proveedor.

b. Llevar a cabo actividades de consulta técnica que podrían incluir análisis de deficiencias/ajustes, revisiones de diseño del sistema, evaluaciones de compatibilidad de dispositivos, revisiones de diseño funcional y técnico, así como revisiones de rendimiento de la USP del proveedor.

c. Realizar una evaluación del sistema y garantizar el cumplimiento de las mejores prácticas de la USP del proveedor.

d. Proporcionar una estrategia de migración y actualización para la USP del proveedor según corresponda.

e. Proporcionar documentación con relación a la arquitectura del sistema, el diseño del sistema, las especificaciones de hardware y los requisitos de compatibilidad, los cálculos del ancho de banda de las cámaras y las mejores prácticas con respecto a la USP del proveedor.

D. Servicio de Configuración y Puesta en Marcha de Sistemas:

1. La Configuración del Sistema y el Servicio de Puerta en Marcha del proveedor deberá incluir un Ingeniero de Campo quien será responsable por:

a. Asistir a los técnicos en el lugar/remotos del contratista o subcontratista con la configuración y puesta en marcha de la USP del proveedor en el sitio del cliente.

b. Llevar a cabo una prueba de la USP después de la instalación del sistema usando escenarios del operador reales para asegurar un desempeño óptimo del sistema.

c. Proporcionar al contratista con un Informe de Servicio que indique con detalle las tareas realizadas durante la integración de la USP en el sitio del cliente, al igual que recomendaciones para mejorar el desempeño de la USP que deben ser implementadas por el contratista.

d. Proporcionar una transferencia de conocimiento de la USP del proveedor al contratista después de la implementación de la USP en el sitio del cliente.

3.04 Capacitación del operador usuario final del fabricante *(Prescriptor, este es un cobro de medio día más gastos)*

A. El contratista deberá contratar los servicios del proveedor de la USP para asistir en la capacitación del usuario final de la USP en el sitio final del usuario.

FIN DE LA SECCIÓN

Sección 28 19 00 – Sistema de Identificación del Control de Acceso de Vehículos

Parte 1 - Información General

1.01 Trabajo relacionado

A. Sección 28 13 00 – Sistema Electrónico de Control de Acceso

B. Sección 28 23 00 – Videovigilancia

C. Sección 28 51 00 – Gestión y Presentación de la Información

1.02 Definiciones

A. ACS - Sistema de Control de Acceso

B. ALPR – Reconocimiento Automático de Placas de Matrícula

C. CSA - Aplicación de Software del Cliente

D. DGM - Mapas Gráficos Dinámicos

E. SDK - Kit de Desarrollo del Software

F. SSM - Módulo de Software del Servidor

G. UI - Interfaz de Usuario

H. USP - Plataforma Unificada de Seguridad

I. UWC - Cliente Web Unificado

J. VMS - Sistema de Administración de Videos

1.03 Requisitos

A. El programador del sistema deberá haber asistido a la capacitación del fabricante y obtenido la Certificación Técnica en Security Center - AutoVu™ de Genetec™.

B. Como opción, el programador del sistema deberá haber asistido a la capacitación del fabricante y obtenido la Certificación Técnica en Security Center - Enterprise de Genetec.

C. El programador del sistema deberá ser un Socio de Negocios Certificado Genetec con el siguiente nivel de preparación: *(Especificador: seleccione una de las siguientes opciones)*

1. Socio de Negocios Certificado o superior
2. Socio de Negocios Élite o superior
3. Socio de Negocios Élite Unificado

D. El programador del sistema deberá presentar comprobante de las certificaciones.

Parte 2 - Productos

2.01 Cámaras todo en uno SharpV

A. Equipo diseñado para proporcionar funcionalidad de reconocimiento automático de placas de matrícula (ALPR, por sus siglas en inglés).

B. En cada unidad, dos cámaras, una fuente de iluminación y un procesador.

C. Comunicación con las unidades por medio de Ethernet.

D. El motor ALPR se puede localizar para mejorar el rendimiento.

E. Base de datos de contextos internacionales disponible.

F. Cámara ALPR monocromática CCD de alta resolución (1280 X 960, 1,2 Mpx) con escaneado progresivo.

G. Objetivo focal variable apto para 8,5 mm a 50 mm.

H. Iluminación infrarroja pulsada para la lectura automática de alto rendimiento de placas de matrícula (ALPR).

I. Control automatizado de la exposición basado en las indicaciones del motor ALPR.

J. Cámara a color de alta resolución (1280 X 960, 1,2 Mpx) con escaneado progresivo para grabación de videos y visualización general de imágenes

K. Objetivo focal variable con capacidad de opción de alcance estándar: 5 a 10 mm (hasta 65 ft/20 m), u opción de largo alcance: 12,5 a 50 mm (hasta 105 ft/32 m).

L. Hardware de captura de video integrado.

M. Entradas/salidas optoaisladas duales.

N. Tasa de procesamiento de 30 cuadros por segundo.

O. Recinto robusto sellado, y cableado diseñado para aplicaciones fijas.

P. Almacenamiento integrado de datos leídos en caso de pérdida de la red.

Q. Región de Interés para realizar el ALPR en un polígono recortado dentro del campo de visión (FOV, por sus siglas en inglés).

R. Capacidades de codificación de video: MJPEG, 15 FPS, 1280 X 960 (1,2 Mpx).

S. Interfaz de red: 1 puerto Ethernet Base-T 10/100/1000.

T. Preprocesamiento avanzado de imágenes de hardware que permite el reconocimiento de placas de matrícula a una tasa completa de cuadros del sensor.

U. Disponible en negro o blanco de seguridad

V. Procesador: Intel Atom E3845 de cuatro núcleos y 1,91 GHz (2 MB de caché L2) y 4 GB de RAM.

W. Sistema operativo: Windows 10 Enterprise.

X. Iluminación pulsada a base de LED: Alcance de 20 m (estándar) o de 32 m (de largo alcance).

Y. Iluminación pulsada a base de LED: Longitudes de onda de 850 nm y 740 nm disponibles.

Z. Resistente a alteraciones con ventana frontal a prueba de golpes.

AA. Incluye montaje de panoramización / inclinación Videotec y adaptador Pelco.

BB. Temperatura de funcionamiento de -40 °F a 149 °F (de -40 °C a 65 °C)

CC. Temperatura de almacenamiento: -40 °F a 185 °F (-40 °C a 85 °C)

DD. Sellado: A prueba de agua según IP66/67 (1 m de inmersión durante 48 horas).

EE. Fuente de alimentación: Alimentación a través de Ethernet (PoE+, por sus siglas en inglés) 802.3at Tipo 2 (25,5 W).

FF. Dimensiones: 2,5 X 7,6 X 8,5 pulgadas (63 X 192 X 214 mm).

GG. Peso: 5,04 lb (2,29 kg).

2.02 Aplicación del Software del Cliente

A. Las CSA se fusionarán continuamente con el reconocimiento automático de placas (ALPR) y con las funcionalidades de video dentro de la misma aplicación del usuario. El VMS deberá ofrecer una solución completa y escalable de videovigilancia que deberá permitir la adición de cámaras sobre bases unitarias.

B. El CSA deberá soportar la capacidad de seleccionar varias regiones en un mapa y proporcionar resultados que sean comunes a todas las regiones.

C. El CSA permitirá que usuario evite la eliminación de una lectura o acierto durante un periodo de tiempo configurable.

D. El CSA permitirá que el usuario corrija manualmente una lectura de placas.

E. El CSA presentará al usuario un Asistente sencillo para la creación de listas activas

F. El CSA permitirá que el usuario cree una lista activa sin necesidad de ninguna otra información de atributos, distinta del número de matrícula.

G. El CSA permitirá que el usuario busque en las listas de acceso configuradas, cualquier información en cualquiera de los campos especificados.

H. El CSA permitirá que el usuario genere un informe de lectura específicamente dirigido a aquellas lecturas que generaron un acierto.

I. El CSA permitirá la visualización basada en mapas del monitoreo de lecturas en tiempo real.

J. El CSA permitirá que el usuario busque números de matrícula completos o parciales.

K. El CSA permitirá que el usuario busque números de matrícula usando comodines.

L. La CSA deberá permitir que el usuario automatice la descarga de Listas Activas desde un servidor FTP/SFTP o HTTP/HTTPS utilizando la autenticación de nombre de usuario/contraseña/certificado.

M. El CSA permitirá que el usuario personalice el formato de los informes mostrados en pantalla.

2.03 Interfaz de usuario de vigilancia (UI)

A. El IU de vigilancia proporcionará una interfaz para soportar las siguientes tareas y capacidades de ALPR:

1. Monitoreo y administración de eventos ALPR y alarmas.
2. Visualización de foto(s) de placas de matrícula e imágenes de contexto.
3. Visualización de información de placas de matrícula (por ejemplo, lecturas de las placas de matrícula)
4. Verificación de datos ALPR contra video en vivo y grabado.

2.04 Requisitos de la Interfaz de Usuario del Administrador del Servidor

A. El Administrador del Servidor se usará para configurar el SSM y la Función de Directory (configuración principal) y su(s) base(s) de datos para aplicar la licencia, y otros más.

B. El Administrador del Servidor será una aplicación basada en la Web. A través del Administrador del Servidor será posible tener acceso al SSM a lo largo de la red o de forma local en el servidor.

C. El acceso al Administrador del Servidor estará protegido a través de un nombre de inicio de sesión, contraseña y comunicaciones encriptadas.

D. El Administrador del Servidor deberá permitir al administrador (usuario) realizar las siguientes funciones:

1. Administrar la licencia del sistema.
2. Configurar la(s) base(s) de datos y el servidor de la base de datos para la Función de Directory.
3. Activar/Desactivar la Función de Directory
4. Respaldar manualmente la(s) base(s) de datos de la Función de Directory y/o restaurar la(s) base(s) de datos del servidor, al igual que configurar las copias de seguridad programadas de las bases de datos.
5. Definir las configuraciones de seguridad de las comunicaciones entre el cliente y el servidor.

6. Configurar el hardware de comunicaciones de la red, incluidos las direcciones y los puertos de conexión.
7. Configurar las configuraciones SMTP del sistema (servidor de correo y puerto).
8. Configurar opciones de almacenamiento de historial de eventos y alarmas.

2.05 Requisitos Generales del Unified Web Client (UWC)

A. La USP deberá soportar un cliente web unificado (UWC, por sus siglas en inglés) para el control de acceso, los videos y el reconocimiento automático de placas de matrícula.

B. La UWC deberá ser un cliente verdaderamente ligero que no requiera de ninguna descarga con excepción de un navegador de web o plugins estándar de navegador de web.

C. La UWC deberá ser independiente de plataformas y ejecutarse dentro de Internet Explorer de Microsoft, Firefox, Safari y Google Chrome.

D. El UWC deberá diseñarse como una aplicación HTML5.

E. El UWC deberá soportar la visualización en formato de tableta.

F. El UWC deberá soportar videos nativos H.264 en el cliente web.

G. Las páginas web para el Web Client serán administradas e insertadas por el servidor Web Client. No será necesario Microsoft IIS ni ningún otro servicio de hospedaje de sitios web debido a que todas las páginas web serán hospedadas por el Mobile Server.

H. El Web Client Server deberá proporcionar la capacidad de definir una URL única para acceder al Web Client, a fin de garantizar la seguridad de la aplicación.

I. El UWC proporcionará la capacidad de cargar un plano de cámara.

J. El UWC proporcionará la habilidad de configurar, guardar y volver a cargar los diagramas privados de la cámara.

K. El UWC proporcionará la habilidad de controlar las Cámaras PTZ.

L. Funcionalidades:

1. El soporte para iniciar sesión estará disponible mediante:
    a. Nombre de usuario y contraseña
    b. Active Directory *(Specifier, Professional y superior, se requiere licencia adicional para Active Directory)*
    c. Proveedor de identidad Azure Active Directory, ADFS, OpenID Connect o SAML2 *(Especificador, Profesional y superior, se requiere licencia adicional para OIDC y SAML2)*
2. Capacidad del usuario de cambiar su contraseña.

3. Encriptar las comunicaciones para todas las transacciones.
4. Impresión de informes y exportación a un archivo CSV.
5. Control de acceso:
    a. Tarjetahabiente y grupo (agregar/modificar/borrar)
    b. Administración de credenciales (agregar/modificar/eliminar)
    c. Administración de reglas de acceso (agregar/modificar/eliminar)
    d. Administración de visitantes (registro de entrada/modificación/registro de salida)
    e. Desbloqueo de puerta
    f. Anulación del horario de desbloqueo de una puerta
    g. Informe de Actividades de Puertas
6. Alarmas
    a. Informe de alarma
7. Administración de los Niveles de Amenaza
8. Reconocimiento Automático de Placas de Matrícula (ALPR)
    a. Monitoreo en vivo de las cámaras ALPR
    b. Informe de lecturas y aciertos de ALPR
    c. Registro de números de placas de matrícula en listas activas

2.06 Monitor de salud

A. La USP deberá monitorear el estado de salud del sistema, los eventos relacionados con los registros del estado de salud y calcular estadísticas.

B. Los servicios de la USP, funciones, agentes, unidades y aplicaciones de clientes activarán los eventos de los estados de salud.

C. La USP deberá llenar el Registro de Eventos Windows con eventos del estado de salud relacionados con las funciones de la USP, servicios y aplicaciones de clientes.

D. Una función exclusiva, la Función de Monitoreo del Estado de Salud, deberá realizar las siguientes acciones:

1. Monitorear el estado de la salud de todo el sistema y los eventos de registros.
2. Calcular estadísticas dentro de un marco de tiempo específico (horas, días, meses).
3. Calcula la disponibilidad para clientes, servidores y unidades de ALPR/acceso/video.

E. Una tarea de Monitoreo del Estado de Salud y una tarea de generación de informes del Historial del Estado de Salud deberá estar disponible para la generación de informes en vivo y de historiales.

F. En la interfaz de usuario de la aplicación cliente, una tarea del tablero de control correspondiente al Monitoreo del Estado de Salud para proporcionar información en vivo, como gráficos circulares y listas de eventos, con el objetivo de evaluar de forma rápida y visual la salud general del sistema.

G. Un tablero de control del estado de salud centralizado basado en la web deberá estar disponible para visualizar las unidades y eventos de funciones del estado de salud de la USP de manera remota.

H. Estadísticas detalladas del cuidado del sistema estarán disponibles a través de un tablero de control basado en la web, y proporcionará métricas del estado de salud de las entidades y funciones de la USP, incluyendo tiempo activo y tiempo promedio entre fallas.

I. Todos los eventos de salud generados en el sistema se pueden usar para automatizar la administración de eventos y acciones de la USP.

J. Los eventos del estado de salud serán accesibles a través del SDK (puede usarse para crear capturas de SNMP).

2.07 Requisitos Generales de la USP

A. La Plataforma Unificada de Seguridad (USP) deberá ser una solución de software clase empresarial de seguridad y protección habilitada para IP.

B. El USP soportará la unificación continua del Sistema Automático de Reconocimiento del placas IP (ALPR), el sistema de control de acceso IP (ACS) y el sistema de gestión de video IP (VMS) bajo una sola plataforma. Las aplicaciones de interfaz de usuario (UI) de la USP presentarán una interfaz unificada de seguridad para la administración, configuración, monitoreo y generación de informes de los sistemas embebidos ALPR, ACS y VMS, y dispositivos periféricos asociados.

C. Las funcionalidades disponibles con la USP deberán incluir:

1. La configuración de sistemas embebidos, como los sistemas ALPR, ACS, y VMS.

2. El monitoreo de eventos en vivo.

3. El monitoreo de video en vivo y reproducción de video archivado.

4. Administración de alarmas.

5. La generación de informes que incluyan la creación de plantillas de informes personalizados e informes de incidentes.

6. La característica de Federation para el monitoreo global, los informes, y la administración de alarmas de múltiples sistemas ALPR, ACS y/o VMS remotos e independientes esparcidos a lo largo de múltiples instalaciones y zonas geográficas. *(Especificador, solo Enterprise, se requiere licencia adicional)*

7. La administración global de tarjetahabientes a lo largo de múltiples instalaciones y zonas geográficas, cada una con su propio sistema ACS independiente. *(Especificador, solo Enterprise, se requiere licencia adicional para cada sitio)*
8. Integración de Microsoft Active Directory para la sincronización de las cuentas de usuarios de la USP y cuentas de tarjetahabientes del ACS. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
9. Dispositivo de intrusión e integración de paneles (monitoreo en vivo, generación de informes y armado/desarmado). *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
10. Integración de los dispositivos de Intercomunicador SIP para comunicación bidireccional. *(Especificador, todas las versiones, se requiere licencia adicional)*
11. Integración con sistemas y bases de datos de terceros a través de plug-ins (control de acceso, analíticas de video, puntos de venta, y otros.). *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
12. Visualización de mapas gráficos dinámicos.
13. Integración del sistema de administración de activos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

D. La USP deberá ser instalada en uno o más de los siguientes tipos de instalaciones:

1. ALPR unificado, accesos, plataforma de videos y cualquier combinación de ellos.
2. ALPR independiente, control de acceso o plataforma de videos.
3. Acceso unificado y plataforma de video que federa con múltiples ALPR, ACS y VMS remotos.
4. Plataforma independiente de video que federa múltiples ALPR remotos independientes.
5. Plataforma independiente de video que federa múltiples VMS remotos independientes.
6. Control de acceso independiente que federa múltiples ACS remotos independientes.

E. Concesión de licencias:

1. Se deberá aplicar una sola concesión de licencias central en el servidor de configuración.
2. No deberá existir un requisito de aplicar una licencia en todo servidor de computadora o estación de trabajo de cliente.
3. Con base en las opciones seleccionadas, se podrán habilitar o deshabilitar uno o más sistemas embebidos.

F. Requisitos de Hardware y Software:

1. Los sistemas USP y embebidos (reconocimiento de placas de matrícula, control de acceso y video) estarán diseñados para ejecutarse en una plataforma estándar basada en PC equipada con el sistema operativo Windows. El sistema operativo preferido deberá ser coordinado con el Propietario siguiendo los sistemas operativos soportados por el fabricante.
2. El software básico del cliente/servidor será desarrollado en su totalidad usando la plataforma de software .NET de Microsoft y el lenguaje de programación C# (C-Sharp).
3. El(los) servidor(es) de base de datos de la USP deberá(n) estar desarrollado(s) sobre el Servidor SQL de Microsoft. La versión SQL preferida deberá coordinarse con el Propietario y ser compatible con la USP.
4. La USP deberá ser compatible con los ambientes virtuales, incluyendo VMware y Microsoft Hyper-V.
5. La USP deberá usar el desarrollo y las tecnologías de programación más recientes de interfaz de usuario (UI) como lo son Microsoft WPF (Windows Presentation Foundation), el lenguaje de marcado XAML, y la plataforma de software .NET.

2.08 Arquitectura de la USP

A. La USP estará basada en un modelo de cliente/servidor. La USP deberá consistir de un Módulo de Software de Servidor (SSM) estándar y Aplicaciones de Software del Cliente (CSA).

B. La USP deberá ser una solución habilitada para IP. Toda la comunicación entre el SSM y la CSA estará basada en el protocolo TCP/IP estándar y deberá usar la encriptación TLS con certificados digitales para proteger el canal de comunicación.

C. El SSM deberá ser un servicio Windows que se pueda configurar para que comience a funcionar cuando se inicia y ejecuta el sistema operativo en el fondo. El SSM deberá comenzar a funcionar automáticamente cuando se enciende la computadora sin importar si hay o no un usuario con sesión iniciada en la máquina.

D. Los usuarios podrán implementar el SSM en un solo servidor o a lo largo de varios servidores para una arquitectura distribuida. La USP no tendrá restricciones en cuanto al número de SSM instalados.

E. La USP soportará el concepto de la característica de Federation en donde se pueden enlazar múltiples instalaciones independientes ALPR, ACS y VMS en un solo sistema virtual grande para el monitoreo, la generación de informes y la administración de alarmas centralizados. *(Especificador, solo Enterprise, se requiere licencia adicional)*

F. La USP deberá proteger contra la posible falla del servidor de la base de datos y continuar funcionando con soluciones estándar disponibles en el mercado .

G. La USP deberá soportar hasta mil instancias de CSA conectadas al mismo tiempo. Sin embargo, se puede instalar un número ilimitado de CSA en cualquier momento. *(Especificador, máximo 5 con Standard; máximo 10 con Professional; ilimitado con Enterprise)*

H. La USP deberá soportar un número ilimitado de registros e historial de transacciones (eventos y alarmas) con el máximo permitido limitado por la cantidad de disco duro disponible.

I. La USP deberá soportar la transmisión de video sin interrupción. La CSA deberá mantener las conexiones de video existentes activas en caso de que un SSM (con excepción del Archiver) no esté disponible.

J. Arquitectura con Base en Funciones:

1. La USP deberá consistir de una arquitectura con base en funciones, donde cada SSM hospeda una o más funciones.
2. Cada función ejecutara un conjunto específico de tareas relacionadas, ya sea con el sistema principal, el reconocimiento automático de licencias (ALPR), el control de acceso (ACS), o las funcionalidades de video (VMS), entre muchas otras. La instalación deberá estar simplificada a través de la habilidad de la USP para permitir a los administradores:
    a. Instalar uno o varios SSM a lo largo de la red antes de activar las funciones.
    b. Activar y desactivar funciones según sea necesario en cada SSM.
    c. Centralizar la configuración y administración de la función.
    d. Soporte de configuración remota.
    e. Mover las funciones desde un SSM a otro.
3. Cada función, cuando sea necesario, deberá tener su propia base de datos para almacenar eventos e información de configuración específica a la función.
4. Las funciones sin base de datos, como la característica de Federation, Active Directory, y la Administración Global de Tarjetahabientes, deberán admitir el modo de espera muy próximo al tiempo real sin que se requiera software de conmutación por error de terceros.
5. Función de Directory
    a. La Función de Directory deberá administrar la base de datos central que contiene toda la información del sistema y la configuración de componentes de la USP.
    b. La Función de Directory deberá autenticar usuarios y dar acceso a la USP con base en derechos o privilegios de acceso predefinidos del usuario y configuraciones de particiones de seguridad.
    c. La función de Directory soportará la configuración/gestión de los siguientes componentes comunes a los subsistemas del ALPR, ACS y VMS:
        i. Particiones de seguridad, usuarios y grupos de usuarios
        ii. Áreas
        iii. Zonas, reglas de enlace de entrada/salida (E/S) y comportamiento de salida personalizado

iv. Alarmas. Horarios y tareas programadas

v. Eventos personalizados

vi. Macros o guiones personalizados

d. La función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al ALPR:

i. Unidades y cámaras ALPR

ii. Listas activas, listas de permisos y reglas de sobretiempo

e. La función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al ACS:

i. Controladores de puertas, y módulos de entrada y salida (E/S)

ii. Puertas, Elevadores y Reglas de acceso

iii. Tarjetahabientes y grupos de tarjetahabientes, credenciales y plantillas para distintivos

f. La función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al VMS:

i. Servidores de video y sus periféricos (como audio, E/S y puertos serie)

ii. PTZ.

iii. Secuencias de cámaras

iv. Horarios de grabación y archivamiento

6. La Función del Reconocimiento Automático de Placas de Matrícula (ALPR) será responsable de sincronizar las unidades fijas ALPR (cámaras) y aplicaciones ALPR móviles bajo su control. La Función de ALPR será responsable de registrar todas las actividades y eventos del ALPR.

7. La función del Video Archiver será responsable de administrar las cámaras y los codificadores que controle y archive.

8. La función del Media Router será responsable de enrutar los flujos de video y audio en redes locales y de área extensa, desde la fuente (como el DVS) hacia el destino (como la CSA).

9. La función del Administrador de Acceso será responsable de la sincronización de las unidades de hardware de control de acceso bajo su control, como lo son los controladores de puerta y los módulos de E/S. Además esta función debe ser responsable de validar y registrar todas las actividades y eventos de acceso cuando los controladores de puertas y los módulos E/S están en línea.

10. La Función de Zone Manager será responsable de administrar todas las zonas de software (recopilación de entradas) y el registro de eventos de zona asociados. Las zonas deberán consistir de entradas de control de acceso y de dispositivos de video.

11. La Función de Monitoreo del Estado de Salud será responsable por el monitoreo y registro de eventos y advertencias del estado de salud desde varias aplicaciones de cliente, funciones, y servicios que forman parte de la USP. Esta función también será responsable de registrar eventos dentro del Windows Event Log y por generar informes sobre las estadísticas y el historial de salud.
12. Funciones Opcionales:
    a. La característica de Federation será responsable de crear un gran sistema virtual que consista de cientos o miles de sistemas ALPR, ACS y/o VMS independientes y remotos. *(Especificador, solo Enterprise, se requiere licencia adicional)*
    b. La Función del Global Cardholder Synchronizer será responsable de sincronizar la información de los tarjetahabientes y las credenciales entre el sitio local y el sitio central. También deberá soportar la sincronización entre sitios remotos. *(Especificador, solo Enterprise, se requiere licencia adicional)*
    c. La Función del Active Directory será responsable de sincronizar las cuentas de los usuarios y las cuentas de los tarjetahabientes con un servidor Microsoft Active Directory. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
    d. La Función del Intrusion Manager será responsable de administrar los dispositivos de intrusión de terceros tales como los paneles de alarmas y los dispositivos de detección de perímetros. Esta función también será responsable de registrar de todos los eventos de intrusión en una base de datos. *(Especificador, Standard, Professional y versiones superiores, se requiere licencia adicional)*
    e. La función del Asset Manager será responsable de integrar y sincronizar los sistemas de administración de activos de terceros y eventos relacionados con el registro de activos. La función será responsable de soportar la ejecución de informes relacionados con activos como informes de inventarios e informes de actividad de activos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
    f. La función del Plugin Manager deberá ser responsable de la comunicación entre la USP y los sistemas de terceros, como sistemas de video analíticas, ALPR, control de acceso, video y administración de edificios. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
    g. La Función del Point of Sale (POS, por sus siglas en inglés) será responsable de integrar la USP con los sistemas POS de terceros y de registrar las transacciones. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
    h. La Función de Web SDK será responsable de conectar la USP a cualquier aplicación o interfaz desarrollada con el Web Service SDK. Las aplicaciones desarrolladas con el Web Service SDK serán independientes de la plataforma y dependerán del protocolo REST para las comunicaciones. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

i. La Función Communication Management será responsable de registrar los extremos de comunicación SIP y de administrar el enrutamiento de las llamadas. *(Especificador, todos los paquetes, se requiere licencia adicional)*

j. La función del Video Redirector deberá ser responsable de conectar cualquier transmisión de video a un sistema de terceros que use el protocolo estándar RTSP. Esta función deberá proporcionar acceso a video en vivo. *(Especificador, Professional y versiones superiores, se requieren paquetes de SDK, se requiere licencia adicional)*

K. Servicio de Monitoreo de Servidores (Watchdog):

1. La USP deberá incluir un Servicio de Monitoreo de Servidores que monitoree continuamente el estado del servicio del Módulo de Software del Servidor (SSM).

2. El Servicio de Monitoreo de Servidores será un servicio Windows que se inicia de forma automática en el encender el sistema, sin importar si el usuario está conectado o no a su cuenta.

3. El Servicio de Monitoreo de Servidores estará instalado en todos los servidores y PC que ejecutan un SSM. En caso de fallas o funcionamiento defectuoso, el Servicio de Monitoreo de Servidores deberá reiniciar el servicio averiado. Como último recurso, el Servicio de Monitoreo de Servidores deberá reiniciar el servidor/PC si no fuera posible reiniciar el servicio.

2.09 Unificación de USP ALPR, Video y Control de Acceso

A. El Monitoreo UI presentará una verdadera Interfaz Unificada de Seguridad para la configuración y gestión del ALPR, el ACS y el VMS. La visualización y reproducción avanzada de vídeo en vivo de vídeo archivado deberá estar disponible a través de la UI de Monitoreo.

B. La configuración de UI presentará una verdadera interfaz unificada de seguridad para la configuración y gestión del ALPR, ACS y VMS.

C. El usuario deberá ser capaz de asociar una o más cámaras de video a los siguientes tipos de entidad: cámaras ALPT, áreas, puertas, elevadores, zonas, alarmas, paneles de intrusión y más.

D. Deberá ser posible ver el video asociado con los eventos del ALPR cuando se visualice un informe.

E. La USP deberá soportar la siguiente funcionalidad de la Administración de Alarmas:

1. Crear y modificar alarmas definidas por el usuario. Deberá soportar un número ilimitado de alarmas definidas por el usuario.

2. Asignar un cronograma de tiempo o período de cobertura a una alarma. Deberá activarse una alarma solamente si es una alarma válida para el período de tiempo actual.

3. Establecer el nivel de prioridad de una alarma y su umbral de reactivación.

4. Proporcionar la habilidad de agrupar alarmas por fuente y por tipo.

5. Definir un período de tiempo después del cual se reconoce de forma automática la alarma.
6. Definir los destinatarios de una alarma. Las notificaciones de alarmas deberán distribuirse a uno o más destinatarios. Los destinatarios deberán recibir un nivel de prioridad que jerarquice el orden de recepción de una alarma.
7. Definir el modo de transmisión de la alarma. Las notificaciones de alarmas se enviarán usando un modo de transmisión secuencial o un modo de transmisión de todo a la vez.
8. Definir si se visualiza la fuente de la alarma, una o más entidades o una página HTML.
9. Especificar si es obligatorio la generación de un informe de incidente durante el reconocimiento.

F. Los flujos de trabajo para crear, modificar, agregar instrucciones y procedimientos, y reconocer una alarma deberán ser consistentes para las alarmas ALPR, de control de acceso, y de video.

G. Las alarmas deberán ser federadas, permitiendo la gestión global de alarmas a lo largo de múltiples sistemas independientes ALPR, USP, ACS y VMS.

H. La USP deberá además soportar la notificación de alarmas a una dirección de correo electrónico o a cualquier dispositivo que usa el protocolo SMTP.

I. La habilidad para crear instrucciones relacionadas con las alarmas será soportada a través de la visualización de una o más páginas HTML después de un evento de alarma. Las páginas HTML deberán ser definidas por el usuario y se podrán vincular entre sí.

J. Deberá soportarse el empaque y desempaque de la alarma en donde todas las entidades relacionadas con una alarma se puedan visualizar en la UI de Monitoreo con un simple clic de un botón.

K. El usuario tendrá la habilidad de reconocer alarmas, crear un incidente al reconocer una alarma, y colocar una alarma en el modo repetición.

L. El usuario deberá ser capaz de activar alarmas de forma espontánea según lo que vea en el sistema.

M. Una alarma deberá estar configurada de tal forma que permanezca visible hasta que se reconozca la condición de la fuente.

N. El usuario será capaz de investigar la alarma sin tener que reconocerla.

2.10 Niveles de amenaza de la USP *(Especificador: se requiere licencia adicional; solo Enterprise)*

A. La USP deberá soportar los Niveles de Amenaza para cambiar de forma dinámica el comportamiento del sistema para responder a eventos críticos.

B. Los Niveles de Amenaza deberán activarse y desactivarse por el operador de la CSA con el privilegio adecuado.

C. Los Niveles de Amenaza deberán establecerse en un área o en todo el sistema.

D. Los Niveles de Amenaza afectarán el comportamiento del sistema al ejecutar cualquier acción disponible en la USP, como: activar salida, iniciar la grabación, bloquear cámaras, invalidar la calidad de la grabación, armar una zona, colocar una puerta en un modo de mantenimiento, y otros.

E. Se deberá visualizar una notificación visible en toda la CSA del operador cuando se active un Nivel de Amenaza.

2.11 Tarea de la USP remota

A. La USP deberá proporcionar, mediante una Tarea Remota, capacidades para monitorear y controlar de forma remota el contenido de otras estaciones de trabajo que están ejecutando la CSA (UI de Monitoreo) que forman parte del mismo sistema.

B. La USP deberá soportar aplicaciones para paredes de video al conectar y controlar múltiples estaciones de trabajo y monitores de forma simultánea.

C. La Tarea Remota será una interfaz gráfica que muestra la replicación de la estaciones de trabajo remota que están ejecutando la CSA (UI de Monitoreo).

D. La Tarea Remota deberá permitir la conexión a otras estaciones de trabajo que usan un modo de ancho de banda bajo para recibir instantáneas de datos de video visualizado de forma remota.

E. La Tarea Remota deberá permitir la conexión a otras estaciones de trabajo que usan un modo de espía para permanecer invisibles a la estación de trabajo conectada de forma remota. La opción de modo espía deberá estar disponible para los usuarios con permisos para tener acceso a dicha función.

F. La funcionalidad ofrecida por la capacidad de monitoreo y control remoto deberá incluir:

1. Monitoreo remoto y control del monitoreo y las tareas de monitoreo de alarmas.
2. Habilidad para intercambiar cámaras, puertas y zonas de forma remota en los recuadros de visualización.
3. Habilidad para controlar el video en vivo y en reproducción de forma remota.
4. Habilidad para cambiar el patrón del recuadro de forma remota.
5. Habilitad para crear y eliminar tareas de forma remota.
6. Habilidad para iniciar/detener de forma remota los ciclos de las tareas.
7. Habilidad para ir al modo de pantalla completa de forma remota.
8. Habilidad para guardar y volver a cargar el área de trabajo de forma remota.

2.12 Administración Avanzada de Tareas de la USP

A. La USP deberá soportar una infraestructura para administrar las tareas de la UI de Monitoreo que se usan para el monitoreo en vivo, las actividades diarias y la generación de informes.

B. Los administradores deberán ser capaces de asignar tareas y bloquear el área de trabajo del operador. La administración del usuario de su área de trabajo deberá estar limitada por sus privilegios asignados.

C. Los operadores deberán ser capaces de guardar sus tareas ya sea como Tareas Públicas o Tareas Privadas, y en una partición específica. Las Tareas Públicas deberán estar disponibles para todos los usuarios. Las Tareas Privadas solo deberán estar disponibles para el propietario de la tarea.

D. Los operadores deberán ser capaces de compartir sus tareas enviándolas a uno o más usuarios en línea. Los destinatarios deberán tener la opción de aceptar la tarea enviada.

E. Los operadores deberán ser capaces de duplicar una tarea.

2.13 Informes de la USP

A. La USP deberá soportar la generación de informes (informes de base de datos) para el ALPR, el control de acceso, los videos y la intrusión.

B. Cada informe en el sistema deberá ser una tarea de la USP, cada una asociada a su propio privilegio. Un usuario deberá tener acceso a una determinada tarea de informe si cuenta con los privilegios correspondientes.

C. Los flujos de trabajo para crear, modificar, y ejecutar un informe deberán ser consistentes para el ALPR el control de acceso y los informes de video.

D. Los informes deberán ser federados, permitiendo el informe global consolidado a lo largo de múltiples sistemas independientes USP, ALPR, ACS y VMS.

E. EL ALPR deberá soportar las fotos de las placas de matrícula y el control de acceso deberá soportar las fotos de los tarjetahabientes.

F. La USP deberá soportar los siguientes tipos de informes:

1. Informes específicos de ALPR (reproducción de ALPR móvil, aciertos, lecturas de placas, lecturas/aciertos por día, lecturas/aciertos por zona de ALPR y demás)
2. Informes de alarmas
3. Informes específicos de video (archivos, marcadores, movimiento y otros)
4. Informes de configuración (tarjetahabientes, credenciales, unidades, reglas de acceso, lectores/entradas/salidas y más)
5. Informes de actividades (tarjetahabientes, grupo de tarjetahabientes, visitantes, credenciales, puertas, unidades, áreas, zonas, elevadores y más)

6. Informes de actividad del estado de salud y estadísticas del estado de salud
7. Otros tipos de informes, como informes de visitantes, informes de registros de auditoría, informes de incidentes e informes de horario y asistencia

G. Informes Genéricos, Informes Personalizados y Plantillas de Informes

1. El usuario deberá tener la opción de generar informes genéricos desde una lista existente, generar informes desde una lista de plantillas definidas por el usuario, o crear un nuevo informe o una plantilla de informe.
2. El usuario deberé ser capaz de personalizar informes predefinidos y guardarlos como nuevas plantillas de informe. No existirá la necesidad de una herramienta externa de generación de informes para crear informes personalizados y plantillas de informe. Las opciones de personalización incluirán la configuración de filtros, extensión del informe, y período de tiempo de espera. El usuario también deberá ser capaz de establecer cuales columnas serán visibles en un informe. La clasificación de los datos reportados estará disponible haciendo clic en la columna correspondiente y seleccionando un criterio de clasificación (ascendente o descendente).
3. Todas las plantillas de informes deberán crearse dentro de la UI de Monitoreo.
4. Estas plantillas se pueden usar para generar informes sobre un cronograma en formato PDF o Excel.
5. Un número ilimitado de informes y plantillas personalizadas serán soportados.

H. El diagrama de una tarea de generación de informes deberá consistir de paneles con configuraciones (duración de informe, filtros, mandos ‘ir a’ y ‘restablecer’, etc.), los datos actuales del informe en formato de columna, y un panel con recuadros de visualización. El usuario deberá ser capaz de arrastrar y soltar registros individuales en un informe sobre uno o más recuadros de visualización para ver un evento ALPR, la foto de identificación de un tarjetahabiente o la reproducción de una secuencia de video.

I. La USP deberá soportar el filtrado completo de datos para la mayoría de los informes con base en el tipo de entidad, tipo de evento, marca de tiempo del evento, campos personalizados, etc.

J. La tarea de informe tendrá la capacidad de mostrar resultados a través de gráficos, como gráficos de líneas, gráficos de barras, gráficos de barras apiladas, gráficos de anillos y gráficos circulares.

K. El usuario deberá ser capaz de hacer clic sobre una entidad dentro de un informe existente para generar informes adicionales desde la UI de Monitoreo.

L. La USP deberá soportar las siguientes acciones en un informe: imprimir el informe, exportar el informe a un archivo PDF/Microsoft Excel/CSV, exportar los gráficos en formato JPG/PNG y enviar de manera automática por correo electrónico un informe en función de un horario y una lista de uno o más destinatarios.

2.14 Tableros de la USP

A. La USP deberá ser capaz de crear tableros.

B. Los operadores deberán poder ver los tableros si cuentan con los privilegios correspondientes. Los usuarios con los privilegios correspondientes también deberán ser capaces de modificar los tableros.

C. Los tableros del sistema deberán ser una tarea de la USP. Un usuario deberá tener acceso a una tarea específica de tablero si cuenta con los privilegios correspondientes.

D. Los tableros se deberán guardar en una carpeta privada o pública.

E. Un tablero deberá estar formado por un área de trabajo con varios widgets que aparezcan en dicha área. Todos los widgets deberán proporcionar la capacidad de especificar su ubicación y tamaño, un título y un color de fondo, y de ofrecer la capacidad de actualizar su contenido con frecuencia.

F. Tipos de widgets para tableros:

1. Imagen: ofrece la capacidad de mostrar una imagen (JPG, PNG, GIF y BMP) en un tablero.

2. Texto: ofrece la capacidad de mostrar texto en un tablero. El estilo del texto deberá poder configurarse, de manera que el usuario pueda especificar la fuente, el tamaño, el color y la alineación.

3. Mosaico: ofrece la capacidad de mostrar una URL en un tablero.

4. Página web: ofrece la capacidad de mostrar una URL en un tablero.

5. Cantidad de entidades: ofrece la capacidad de mostrar la cantidad total de un determinado tipo de entidad en la USP.

6. Informes: ofrece la capacidad de mostrar los resultados de los informes guardados en el sistema. Los resultados se visualizarán mostrando la cantidad total de resultados en el informe, un conjunto de los principales resultados del informe o un gráfico visual de los datos del informe.

G. Será posible ampliar los widgets de un tablero con un SDK. De esta forma, se podrán desarrollar widgets personalizados para el sistema.

H. La USP deberá soportar las siguientes acciones en un tablero: imprimir el tablero, exportar el tablero a un archivo PNG y enviar automáticamente por correo electrónico un informe en función de un horario y una lista de uno o más destinatarios.

2.15 Característica de Federation de la USP: Monitoreo de sistemas remotos *(Especificador: solo Enterprise, licencia adicional obligatoria para cada sitio y entidad federada.)*

A. La USP soportará el concepto de Característica de Federación para ALPR, control de acceso y video.

B. La característica de Federation permitirá la unificación de múltiples sistemas USP independientes (sistemas Federados) en un solo sistema virtual más grande (la característica de Federation). Esto deberá facilitar el monitoreo global de múltiples sistemas USP independientes.

C. La característica de Federation deberá soportar la unificación de múltiples sistemas independientes de videovigilancia o VMS.

D. Las entidades que se federarán y monitorearán de forma centralizada desde la característica de Federation deberán incluir eventos ALPR, alarmas, áreas, cámaras, tarjetahabientes y grupos de configuración de tarjetahabientes, credenciales, puertas, elevadores y zonas (entradas monitoreadas).

E. La característica de Federation deberá soportar una integración basada en nube, por medio de la cual se actualizarán de forma automática el servicio e infraestructura y la proporcionará el proveedor del servicio, sin la necesidad de hardware en el sitio.

F. La característica de Federación deberá soportar la Gestión Global de Alarmas desde la UI de Monitoreo para ALPR, control de acceso y video.

G. La característica de Federación deberá soportar la Generación Global de Informes desde la UI de Monitoreo para ALPR, control de acceso y video.

H. La característica de Federation deberá soportar docenas de acciones del operador en entidades remotas (federadas) desde la UI de Monitoreo (por ejemplo, generar un informe global tomando en cuenta eventos de múltiples sitios independientes o reconocer alarmas remotas).

2.16 Administración de Seguridad del Usuario y Grupo de Usuarios, Particiones y Privilegios de la USP

A. La USP deberá soportar la configuración y la administración de usuarios y grupos de usuarios. Un usuario podrá agregar, borrar o modificar un usuario o grupo de usuarios si cuenta con los privilegios correspondientes.

B. La USP deberá soportar la autenticación de usuario con autenticación basada en notificaciones usando proveedores externos. Los proveedores externos deberán incluir:

1. ADFS (Servicios de federación de Active Directory)
2. Azure Active Directory (a través de OpenID Connect)
3. Ping Identity (a través de OpenID Connect)
4. KeyCloak (a través de OpenID Connect)
5. Otros agentes de autenticación de Open ID Connect/SAML2

C. Los derechos y privilegios de acceso comunes compartidos por múltiples usuarios deberán definirse como Grupos de Usuarios. Los miembros individuales del grupo deberán heredar los derechos y privilegios de sus grupos de usuarios primario. Se permitirá el anidamiento de grupo de usuarios.

D. Los privilegios del usuario deberán ser amplios en la USP. Todas las entidades configurables para la USP, incluyendo ALPR, control de acceso y video, tendrán privilegios asociados.

E. Entidades específicas, como tarjetahabientes, grupos de tarjetahabientes y credenciales, deberán incluir un conjunto de privilegios más pormenorizado, como el derecho de acceder a campos personalizados y a cambiar la activación o estado del perfil de una entidad.

F. Particiones:

1. La USP deberá limitar lo que pueden ver los usuarios en la base de datos de configuración a través de particiones de seguridad (segmentos de base de datos). El administrador, quien cuenta con todos los derechos y privilegios, tendrá permitido segmentar un sistema en múltiples particiones de seguridad.

2. Todas las entidades que forman parte de la USP se pueden asignar a una o más particiones.

3. Un usuario que reciba acceso a una partición específica solo deberá ser capaz de ver las entidades (componentes) dentro de la partición a la cuál ha sido asignado. El acceso se otorga al asignar al usuario como un usuario aceptado para ver las entidades que forman parte de una partición en particular.

4. Un usuario o grupo de usuarios puede recibir derechos de administrador sobre la partición.

G. Deberá ser posible especificar el usuario y los privilegios del grupo de usuarios con base en la partición.

H. Las opciones avanzadas de inicio de sesión deberán estar disponibles como inicio de sesión doble, y otros.

I. Deberá ser posible especificar un período inactivo para la UI de Monitoreo y después de dicho tiempo la aplicación se bloqueará de forma automática, al mismo tiempo que conserva el acceso a las señales de la cámara visualizadas actualmente.

J. Será posible revisar los permisos de los usuarios y determinar lo siguiente:

1. El usuario o grupo de usuarios que pueden ver o modificar una entidad del sistema.

2. Los privilegios de cada usuario o grupo de usuarios del sistema.

3. El usuario o grupo de usuarios que puede realizar la acción vinculada a un privilegio

2.17 Administración de evento/acción de la USP

A. El USP soportará la configuración y gestión de eventos para ALPR y video. Un usuario será capaz de agregar, eliminar o modificar una acción enlazada a un evento si cuenta con los privilegios correspondientes.

B. La USP recibirá todos los eventos entrantes desde uno o más sistemas ALPR, ACS y/o VMS. La USP deberá tomar las acciones correspondientes con base en relaciones de eventos/acciones definidas por el usuario.

C. La USP deberá recibir y registrar los siguientes eventos:

1. Eventos ALPR
2. Eventos en todo el sistema
3. Eventos de aplicación (clientes y servidores)
4. Eventos de áreas, cámaras, puertas, elevadores y ALPR (lecturas y aciertos)
5. Eventos de unidad
6. Eventos de zona
7. Eventos de alarmas
8. Eventos de monitoreo del estado de salud

D. La USP deberé permitir la creación de eventos personalizados.

E. El USP tendrá la capacidad de ejecutar una acción como respuesta a un evento de ALPR, control de acceso y video. La USP deberá soportar la siguiente lista de acciones, sin estar limitada a:

1. Agregar marcadores
2. Bloquear y desbloquear video
3. Visualizar una cámara en un monitor analógico
4. Visualizar una entidad en la CSA
5. Mandar un informe por correo electrónico
6. Mandar una instantánea por correo electrónico
7. Exportar un informe
8. Ir a la página de inicio
9. Ir a preestablecidos
10. Invalidar la calidad de grabación
11. Reproducir un sonido
12. Reiniciar una unidad
13. Ejecutar una macro
14. Ejecutar un patrón
15. Enviar un mensaje
16. Enviar un correo electrónico

17. Establecer un nivel de amenaza
18. Iniciar/detener la aplicación de protección de video
19. Iniciar / detener grabación
20. Iniciar / detener transferencia
21. Activar alarma
22. Desencadenar una salida

F. La USP deberá permitir que un horario se asocie con una acción. Deberá activarse la acción solamente si es una acción adecuada para el período de tiempo actual.

2.18 Programas y tareas programadas de la USP

A. Horarios:

1. La USP deberá soportar la configuración y la administración de cronogramas complejos. Un usuario podrá agregar, borrar o modificar un horario si cuenta con los privilegios correspondientes.
2. La USP deberá ofrecer total flexibilidad y la capacidad de detallar cuando se crea un cronograma. El usuario deberá ser capaz de definir un cronograma en incrementos de 1 o 15 minutos.
3. Deberán soportarse programas diarios, mensuales, ordinales y específicos.

B. Tareas Programadas:

1. La USP soportará tareas programadas para videos y ALPR.
2. Las tareas programadas deberán ejecutarse en un horario definido por el usuario en un día y hora específico. También deberá soportar tareas periódicas o recurrentes bajo un cronograma.
3. Las tareas programadas deberán soportar todas las acciones estándar disponibles dentro de la USP, como enviar un correo electrónico o enviar un informe por correo electrónico.

2.19 Macros y Scripts Personalizados de la USP

A. La USP habilitará a los usuarios para que automaticen y amplíen las funcionalidades del sistema a través del uso de macros o scripts personalizados para el ALPR, el control de acceso y el video.

B. Los macros personalizados deberán crearse con el Kit de Desarrollo del Software (SDK, por sus siglas en inglés) de la USP.

C. Una macro deberé ejecutarse tanto de forma automática como manual.

D. Se deberá lanzar una macro en la UI de Monitoreo a través de acciones activas.

2.20 Mapas gráficos dinámicos (DGM) de la USP

A. La USP deberá soportar la funcionalidad de mapeo para el control de acceso, videovigilancia, detección de intrusión, ALPR y aplicaciones externas.

B. La USP deberá proporcionar una interfaz centrada en mapas con la habilidad de comando y control de todas las capacidades de la USP desde una interfaz de mapa de pantalla completa.

C. Deberá ser posible extender el mapa sobre todas las pantallas de la estación del cliente de la USP. En el escenario en donde el mapa se extiende sobre todas las pantallas de la estación del cliente de la USP, deberá ser posible navegar el mapa incluyendo panorámica y zoom, y los movimientos del mapa deberán estar sincronizados en todas las pantallas. La expansión del mapa en varias pantallas debe ofrecer las mismas capacidades de mando y control que la visualización en una sola pantalla.

D. Los DGM deberán soportar los siguientes formatos de archivos y protocolos para la importación de los fondos mapas:

1. PDF
2. JPG
3. PNG
4. Servicio de Mosaico de Mapas Web (WMTS, por sus siglas en inglés) y Servicio de Mapas Web (WMS, por sus siglas en inglés) definidos por el Open Geospatial Consortium (OGC)
5. BeNomad
6. AutoCAD (DWG y DXF)

E. El DGM deberá proporcionar los siguientes proveedores de mapas en línea para usar como fondo de mapa y proporcionar la habilidad de administrar su licencia de servicio, si se requiere una:

1. Google Map, aéreo, topografía (Con licencia)
2. Bing Map, aéreo, satélite, híbrido (Con licencia)
3. ESRI ArcGIS (con licencia)
4. Mapa aéreo OpenStreet (con licencia)
5. OVI híbrido

F. Deberá ser posible configurar un conjunto de mapas mixtos elaborados por GIS, proveedores en línea y archivos privados importados, y enlazarlos todos juntos.

G. Los DGM deberán proporcionar la habilidad de visualizar todas las entidades nativas de la USP, entre las que se incluyen:

1. Cámaras, corregir y PTZ

2. Puertas
3. Secuencias de cámaras
4. Áreas
5. Áreas de intrusión
6. Zonas de intrusión
7. Cámaras de reconocimiento de placas de matrícula
8. Entradas digitales
9. Salidas digitales
10. Intercomunicador
11. Alarmas
12. Macros
13. Patrollers de Patrullas Policiales

H. Los DGM deberán proporcionar la habilidad de dibujar y mostrar información sobre el mapa en la siguiente forma:

1. Formas vectoriales: líneas, rectángulos, polígonos y elipses
2. Fotos
3. Texto

I. Los DGM deberán proporcionar la habilidad de visualizar cualquier tipo de entidades de terceros integradas mediante un SDK. *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

J. Los DGM deberán proporcionar la habilidad de mostrar capas de información en el formato Keyhole Markup Language (KML).

K. El DGM deberá proporcionar la habilidad al operador de administrar capas de entidades visualizadas sobre el mapa, y ser capaz de encenderlas y apagarlas y cambiar el orden de superposición.

L. El DGM proporcionará la capacidad para importar capas de datos de uno o más servidores ESRI ArcGIS.

M. La DGM proporcionará a los operadores la capacidad para gestionar capas que son importadas de ESRI ArcGIS. Los usuarios podrán habilitar y deshabilitar las capas, al igual que clasificarlas.

N. Los DGM deberán ofrecer una copia de seguridad y restauración de datos de mapa integrada tanto para los fondos del mapa como para las capas de entidades.

O. Los DGM deberán ofrecer capacidades de conmutación por error.

P. Los DGM deberán ampliarse a varias miles de entidades sobre un solo mapa y cientos de mapas.

Q. Los DGM deberán proporcionar un medio para actualizar el fondo de un mapa sin afectar la configuración del objeto de mapa.

R. Los DGM deberán ofrecer un diseñador de mapas gráficos fácil de usar para configurar los mapas.

S. Los DGM deberán proporcionar una navegación fácil e intuitiva que incluya:

1. La habilidad para crear jerarquías de mapas para facilitar la navegación dentro y entre varios sitios y edificios.
2. La habilidad para definir favoritos para una recuperación de posición recurrente.
3. La posibilidad de crear vínculos entre mapas. Los enlaces de los mapas deberán permitir el vínculo desde un mapa a múltiples mapas que representan los pisos de un edificio. Mantener el nivel de zoom del mapa cuando se navegue por los pisos de un edificio
4. Una experiencia común de usuario en relación a la navegación en el mapa para GIS y para mapas privados. *(Especificador, se requiere Plan Manager Advanced para GIS)*

T. Deberá ser posible monitorear el estado de entidades en el mapa. Deberá ser posible personalizar los íconos de cualquier entidad representada en el mapa.

U. Los DGM deberán ofrecer la habilidad de establecer de forma opcional una notificación de visualización gráfica de la detección de movimiento.

V. Los DGM deberán ofrecer una herramienta inteligente de selección para tener acceso al video. Al hacer clic en la ubicación que el usuario quiere ver, el DGM seleccionará de forma automática las cámaras que pueden ver esta ubicación y mover el PTZ hacia dicha ubicación. Esta herramienta inteligente de selección deberá tomar los obstáculos en consideración y no mostrar las cámaras que no pueden ver la ubicación debido a una pared.

W. Deberá ser posible seleccionar una ubicación dibujando una zona de interés en el DGM, y para visualizar todas las entidades que forman parte de dicha zona de interés a la vez.

X. El usuario deberá ser capaz de seleccionar y visualizar el contenido de múltiples entidades de la USP sobre el mapa en las ventanas emergentes.

Y. El usuario deberá ser capaz de mover, redimensionar y fijar las ventanas emergentes de la entidad USP sobre el mapa.

Z. Deberá ser posible tener acceso a video en vivo y en modo de reproducción desde el mapa.

AA. Deberá ser posible monitorear desde el DGM todas las notificaciones de evento de entidades. Los usuarios podrán encender y apagar las notificaciones por entidad.

BB. Los DGM deberán ofrecer la habilidad de operar completamente la supervisión de alarma. Deberá ser posible:

1. Centrar el mapa sobre entidades relacionadas con la alarma.
2. Visualizar las notificaciones de alarma sobre el mapa y tener acceso a los videos relacionados del mapa.
3. Activar y recibir alarmas.
4. Actuar sobre la alarma desde los DGM, incluyendo reconocimientos, reenvíos e investigación.
5. Visualizar que una alarma ocurrió en un mapa vinculado subyacente.

CC. Los DGM deberán proporcionar las siguientes capacidades de búsqueda:

1. Buscar y centrar por nombre de entidad.
2. Desde la pantalla de una entidad en la USP, ubicar la entidad sobre el mapa y ofrecer la habilidad de seleccionar otra cercana.

DD. Cualquier actualización del contenido de un mapa por parte del administrador deberá ser enviada de forma inmediata y dinámica a todos los usuarios de los DGM.

EE. El DGM deberá soportar el uso de mapas GIS o mapas privados o una combinación de ambos para el fondo del mapa. *(Especificador, se requiere Plan Manager Advanced para GIS)*

FF. El DGM deberá ser compatible con cualquier mapa compatible con GIS con el OGC y con WMTS y WMS de soporte. Esto incluye, más no se limita a, mapas ESRI. El DGM deberá permitir la selección de las capas GIS adecuadas. *(Especificador, se requiere Plan Manager Advanced para GIS)*

GG. Los DGM deberán proporcionar un diseñador de mapas intuitivo para el posicionamiento de la entidad sobre el mapa usando la opción arrastrar y colocar. Cualquier configuración deberá ser gráfica.

HH. Será posible editar y configurar múltiples objetos del mapa a la vez.

II. Todas las modificaciones en el diseño del mapa se conectarán a un registro de auditoría.

JJ. Estarán disponibles varias acciones dentro de los mapas para que se ejecuten con un doble clic simple e intuitivo, con un clic en el botón derecho o la funcionalidad de arrastrar y soltar. Los ejemplos de acciones disponibles a través de los mapas deberán incluir el desbloqueo de puertas y el reconocimiento de una alarma.

KK. Mediante la siguiente funcionalidad, los DGM deberán permitir la administración de alarmas de la USP desde el mapa: *(Especificador: se requiere licencia adicional para Plan Manager Standard y versiones superiores)*

1. Ubicar sobre el mapa entidades relacionadas con la alarma.

2. Mostrar entidades de la alarma con un icono específico, color, nivel de transparencia y velocidad de intermitencia.
3. Listar, seleccionar y ubicar alarmas.
4. Centrado automático del mapa sobre la alarma con mayor prioridad.
5. Manejar la alarma desde el mapa, incluyendo reconocimientos, reenvíos e investigaciones
6. Todos los contenedores del mapa, como puntos activos o enlaces del mapa deberán reflejar el estado de la alarma de las entidades contenidas.

LL. Deberá ser posible agregar funcionalidad avanzada al objeto del mapa usando el SDK. Cualquier funcionalidad disponible mediante el SDK de la USP estará disponible dentro de los mapas. *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

MM. Los DGM deberán ofrecer la herramienta de lazo para:

1. Mostrar entidades en un sitio a través de una sola acción.
2. Activar una acción en todas las entidades de un sitio con un solo clic.
3. Editar múltiples entidades de un solo sitio en forma simultánea.

NN. Los DGM deberán permitir la visualización de las entidades de la USP seleccionadas desde el mapa sobre un monitor remoto (pared de video). *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

OO. El DGM deberá permitir realizar búsquedas en el mapa por nombre de la entidad.

PP. Los DGM deberán permitir el uso de la información KML de mapas superpuestos tanto para mapas GIS como privados. Los objetos movibles deberán estar soportados mediante el uso de KML. *(Especificador, solo Plan Manager Advanced, se requiere licencia adicional)*

QQ. El Contratista deberá proporcionar licencias para cada entidad que requiere ser mostrada en los mapas gráficos. *(Especificador, las licencias se venden en paquetes con base en la cantidad de entidades, especificar la licencia de un sitio o ilimitado después de 1,000 entidades)*

2.21 Auditoría y Registros de Actividades de Usuario de la USP (Registros)

A. La USP deberá soportar la generación de registros de auditoría. Los registros de auditoría deberán consistir de registros de adiciones, eliminaciones y modificaciones del operador/administrador,

B. Los registros de auditoría deberán generarse como informes. Deberán contar con la capacidad de rastrear cambios dentro de períodos de tiempo específicos. También deberá ser posible la consulta sobre usuarios específicos, cambios, entidades afectadas y períodos de tiempo.

C. Para los cambios de configuración de entidades, el informe de registros de auditoría deberá incluir información detallada sobre el valor antes y después de los cambios.

D. La USP deberá soportar la generación de registros de actividades del usuario. Los registros de actividad del usuario consistirán en registros de la actividad del operador en la USP, tales como inicio de sesión, eventos ALPR vistos, ediciones de lista activa, cámaras vistas, impresión de tarjetas de identificación, exportaciones de videos y otros.

E. El ACS soportará las siguientes acciones sobre un informe de registros de auditoría y actividad: impresión y exportación de informes a un archivo PDF/Microsoft Excel/CSV.

2.22 Informes de Incidentes de la USP

A. Los informes de incidentes deberán permitir al operador de seguridad crear informes sobre incidentes que se presentaron durante un turno. Serán soportados los informes de incidentes relacionados con video y los incidentes relacionados con el control de acceso.

B. El operador será capaz de crear informes de incidentes independientes o informes de incidentes enlazados con las alarmas.

C. El operador deberá ser capaz de vincular secuencias múltiples de video a un incidente, tener acceso a los mismos, y cambiar la fecha u hora de las secuencias posteriormente.

D. Deberá ser posible crear una lista de categorías de Incidentes, etiquetar una categoría a un incidente, y filtrar la búsqueda con la categoría como parámetro.

E. Los informes de incidentes deberán permitir la creación de un formulario personalizado sobre el cual se incluya la información sobre un incidente.

F. Los informes de incidentes deberán permitir agregar entidades, eventos y alarmas para soportar las conclusiones del informe.

G. Los informes de incidentes permitirán el uso de un logotipo personalizado, el logotipo predeterminado de Mission Control o ningún logotipo.

2.23 Ingestión de datos de USP

A. La USP deberá permitir la posibilidad de importar datos externos de fuentes externas para mejorar la unificación de las fuentes de datos dentro de la USP.

B. Cada fuente de datos se definirá mediante un conjunto de campos y tipos de campo que describen la fuente de datos. Los tipos de campo serán:

1. Cadena
2. Entero de 32 bits y 64 bits
3. Número de coma flotante
4. Booleano

5. Marca de tiempo
6. Binario (en un archivo o base 64)

C. La visualización de cada punto de datos de una fuente de datos será configurable para determinar qué campos de los datos deben mostrarse. La configuración de cada campo debe ser:

1. Qué campos se muestran u ocultan
2. En qué orden se muestran los campos
3. Una etiqueta para especificar el nombre del campo (en formato clave:valor)
4. Una opción para especificar cómo mostrar el campo (valor de texto, Imagen, valor del portapapeles, hipervínculo a una página web, hipervínculo a una entidad en el sistema, archivo de sonido)

D. Debe haber un privilegio disponible para cada fuente de datos para permitir/denegar el acceso a usuarios y grupos de usuarios específicos de la USP.

E. Los datos ingeridos estarán disponibles en el sistema de informes de la USP.

F. Los datos ingeridos estarán disponibles para mostrarse en los Tableros de control de la USP.

2.24 Integración de terceros de USP

A. Integración de Microsoft Active Directory *(Especificador: se requiere licencia para Professional y versiones superiores)*

1. La USP deberá soportar una conexión directa a uno o varios servidores de Microsoft Active Directory mediante las funciones del Active Directory. La integración del Active Directory deberá permitir la sincronización de información desde el servidor del Active Directory a la USP.
2. La integración del Active Directory deberá permitir la administración central de los usuarios, grupos de usuarios, tarjetahabientes y grupos de tarjetahabientes de la USP.
3. La USP deberá ser capaz de conectarse y sincronizar datos desde múltiples servidores de Active Directory (hasta 10).
4. La USP deberá soportar la sincronización de Grupos Universales del Active Directory al igual que la de grupos de seguridad que pertenecen a otros dominios dentro del mismo bosque.
5. La USP deberá soportar la encriptación del Microsoft Active Directory usando LDAP SSL.
6. Al estar habilitado, el Active Directory deberá administrar el inicio de sesión del usuario a las aplicaciones de la USP del cliente a través de las credenciales Windows del usuario. El inicio de sesión a la USP deberá utilizar características de la administración de contraseña y autenticación nativa del Active Directory.

7. Deberá ser posible sincronizar las siguientes entidades de la USP y su información desde el Active Directory con la USP:
    a. Usuarios (nombre de usuario, nombre y apellido, dirección de correo electrónico y demás)
    b. Grupos de usuarios (nombre del grupo de usuarios, descripción y dirección del correo electrónico del grupo)
    c. Atributos del Active Directory a los campos personalizados de la USP
8. Al estar habilitado, la adición, eliminación o suspensión de la cuenta Windows del usuario en el Active Directory deberá resultar en la creación, eliminación o deshabilitación de la cuenta de usuario equivalente en la USP.
9. Los métodos de sincronización admitidos para adiciones, modificaciones y eliminaciones de entidades sincronizadas deberán incluir en el primer inicio de sesión (solo usuarios), sincronización manual y sincronización programada.
10. La USP deberá soportar las conexiones de los usuarios a través de organizaciones independientes al conectarse a un proveedor de identidad externo mediante una autenticación basada en notificaciones, como ADFS (Active Directory Federation Services), Azure Active Directory, otros proveedores de OpenID Connect y SAML2.

B. Integración de Detección de Intrusión: *(Especificador, Standard, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte el documento de Plugins Compatibles con Security Center)*

1. La USP se deberá integrar con los paneles de intrusión y dispositivos de terceros mediante un SDK de Intrusión. La Función del Intrusion Manager deberá manejar las comunicaciones con los paneles de intrusión. Las comunicaciones con los dispositivos de intrusión deberán ser sobre comunicaciones en serie y/o una red IP.
2. Deberá ser posible la integración con los paneles de intrusión fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.
3. La funcionalidad disponible mediante la integración de dispositivos de intrusión con la USP deberá incluir lo siguiente (en donde sea soportado por el panel de intrusión):
    a. Armar y desarmar dispositivos de intrusión (de forma manual, programada o después de un evento de la USP).
    b. Activación o accionamiento de salidas de dispositivos de intrusión.
    c. Visualización de eventos y alarmas de intrusión.
    d. Vigilancia del estado, incluyendo el estado de armado de los dispositivos de intrusión.
    e. Verificación por video de eventos y alarmas de intrusión con paneles de video.

f. Creación de zonas USP utilizando entradas de dispositivos de intrusión.

C. Sistemas de Control de Acceso de Terceros: *(Especificador, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte la guía de Plugins compatibles con Security Center)*

1. La USP deberá integrarse con software de control de acceso de terceros a través del SDK. Las comunicaciones con software de control de acceso se producirán a través de una red IP y no deberían soportar tareas administrativas como la administración de tarjetahabientes.
2. Deberá ser posible la integración con software de control de acceso fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.
3. La funcionalidad disponible mediante la integración de software de control de acceso con la USP deberá incluir lo siguiente (en donde sea soportado por la solución de control de acceso):
    a. Sincronice entidades de control de acceso y reciba estados y eventos asociados dentro de la USP, lo que incluye:
        i. Derechos de acceso y tarjetahabientes
        ii. Visitantes
        iii. Lectores y puertas
        iv. Alarmas
        v. Entradas y salidas
    b. Monitorear eventos de control de acceso.
    c. Monitorear y reconocer alarmas de control de acceso.
    d. Activar acciones y salidas en el software de control de acceso usando acciones activas y eventos a toma de acción.
    e. Bloquear y desbloquear puertas en el software de control de acceso.
    f. Verificación por video de eventos y alarmas de control de acceso.
    g. Configurar eventos a toma de acción usando los eventos y las alarmas de control de acceso.
    h. Generar informes de Security Center mediante el uso de datos de control de acceso.
    i. Visualizar y monitorear estados de entidades de puertas en los mapas de la USP.
4. Entre los fabricantes de control de acceso actualmente compatibles, se encuentran los siguientes:
    a. Tyco Softwarehouse CCURE
    b. UTC Lenel Onguard

c. Amag Symmetry

d. Siemens Sipass

e. AssaAbloy ARX

D. Integraciones Adicionales de Terceros:

1. La USP deberá soportar enfoques múltiples para la integración de sistemas de terceros. Estas deberán incluir: Kits de Desarrollo de Software (SDK), SDK de Servicio de Web basado en REST, SDK de Servicio RTSP, entre otros. *(Especificador, Professional y versiones superiores, se requiere licencia y paquete SDK)*

2. La arquitectura de la USP deberá soportar la adición de nuevas conexiones para adaptarse a la integración de sistemas de terceros. *(Especificador: Consulte el sitio web para ver cómo se otorgan las licencias)*

3. Integraciones de ALPR con estaciones de pago, proveedores de permisos, proveedores de pagos por teléfono y vendedores de boletos.

4. Información analítica de video

5. Sistemas de video de terceros.

6. Sistemas de control de acceso de terceros.

7. Sistemas de punto de venta (POS).

8. Sistema de administración de edificios.

9. Sistemas de administración de recursos humanos (HRMS).

2.25 Kit de desarrollo de software (SDK) de la USP

A. Un SDK de la USP deberá estar disponible para soportar el desarrollo personalizado para la plataforma.

B. El SDK deberá incluir funcionalidades específicas de los sistemas embebidos de reconocimiento automático de placas de matrícula (ALPR), control de acceso (ACS) y videos (VMS).

C. La integración con aplicaciones y bases de datos externas deberá ser posible con el SDK.

D. El SDK deberá permitir a los usuarios finales desarrollar nuevas funcionalidades (interfaz de usuario, aplicaciones o servicios independientes) para enlazar la USP a sistemas y aplicaciones empresariales de terceros como Sistemas para Uso de Emblemas, Sistemas de Administración de Recursos Humanos (HRMS), y sistemas de Planificación de Recursos Empresariales (ERP).

E. El SDK deberá basarse en la plataforma .NET.

F. El SDK deberá soportar actualizaciones dinámicas y transaccionales a la configuración de la USP. También deberá soportar el cambio de notificación de la configuración de entidad de la USP.

G. El SDK deberá proporcionar una lista completa de las funciones de programación para ver y/o configurar entidades básicas como lo son: usuarios y grupos de usuarios, alarmas, eventos personalizados, cronogramas. etc.

H. El SDK proporcionará una lista completa de funciones de programación para ver y configurar el ALPR, el ACS y el VMS.

I. El SDK proporcionara una lista completa de funciones de programación para ver y configurar la mayoría de las entidades ALPR.

J. El SDK deberá ser capaz de recibir eventos en tiempo real desde las siguientes entidades de la USP: usuarios y grupos de usuarios, áreas, zonas, cámaras, unidades de videos, puertas, controladores de puerta (unidades), elevadores, tarjetahabientes, grupos de tarjetahabientes y credenciales.

K. El SDK deberá ser capaz de consultar el historial de eventos para áreas, cámaras, zonas, alarmas, tarjetahabientes, credenciales, visitantes, puertas, eventos de lectura de consultas de placa de matrícula, eventos de aciertos de placas de matrícula automotriz, generar un informe de aciertos de placa de matrícula , generar un informe de lecturas de placa de matrícula.

L. El SDK deberá soportar las siguientes funciones de alarma: visualización de alarmas en tiempo real, reconocimiento de alarmas, cambiar prioridades y cambiar destinatario.

Parte 3 - Ejecución

3.01 Garantía

A. El producto deberá desarrollarse en todos los aspectos materiales de acuerdo con el manual del usuario adjunto, y los medios en donde resida el Software del Producto estarán libre de defectos en material y mano de obra bajo uso normal. Los defectos de software están cubiertos mediante Lanzamiento de Servicios y Actualizaciones Acumulativas las cuales están disponibles por un 1 año a partir de la fecha de la compra del software.

B. La garantía prolongada, hasta por 5 años, deberá estar disponible mediante la compra del servicio de asistencia de Genetec, el cual incluye los siguientes servicios adicionales además de la garantía estándar:

1. Acceso a soporte telefónico y chat en línea para asistencia técnica.
2. Administración de caso en línea.
3. System Availability Monitor en línea.
4. Acceso a Actualizaciones de Versiones Importantes y Secundarias
5. Soporte de localizador las 24 horas, los 7 días de la semana y especialistas de soporte dedicados. *(Especificador: cargo adicional)*

C. Garantía del Hardware Genetec AutoVu:

1. Todo el hardware de AutoVu incluye un año de garantía de devolución y reparación.
2. Se puede comprar una garantía de reemplazo opcional.
3. La garantía extendida del hardware se puede comprar hasta 5 años a partir de la fecha de la compra.

3.02 Puesta en marcha del sistema y servicios de integración *(Especificador, este es un cobro diario más viáticos, revisar Genetec Inc. para ver el número recomendado de días a especificar)*

A. Requisitos Generales:

1. El contratista deberá ocupar los servicios del integrador de la USP para asistir en la administración de la integración de la USP en el sitio del usuario final en proyectos que involucren:
   a. Varios contratistas o subcontratistas serán responsables por la integración de la USP en varios sitios del cliente en diferentes zonas geográficas.
   b. Instalaciones empresariales complejas que involucran funcionalidad avanzada (por ejemplo, la característica de Federation, conmutación por error, plugins), sistemas múltiples (por ejemplo, control de acceso, video, ALPR) o integraciones de terceros.
   c. El amplio uso de soluciones/plugins personalizados desarrollados por el integrador que se integrarán en la USP.
2. Los servicios del integrador de la USP deberán incluir la Administración de la Integración y Configuración y Puesta en Marcha del Sistema.

B. Servicio de Administración de Implementación:

1. El servicio de Administración de Integración del integrador deberá incluir un Gerente de Proyecto que actúa como el único punto de contacto para todas las comunicaciones entre el contratista y la organización del proveedor quién será el responsable de:
   a. Llevar a cabo la Evaluación de Riesgo del impacto sobre posibles factores de riesgo en el funcionamiento de la USP del integrador.
   b. Proporcionar un plan de proyecto para la integración de la USP del integrador.
   c. Administrar el desarrollo e implementación de los componentes de la solución personalizada que se integrarán a la USP del proveedor (si corresponde).
   d. Proporcionar un ámbito del trabajo que indique en detalle los servicios ofrecidos por el proveedor para asistir en la implementación de la USP del integrador.
   e. Coordinar y programar los servicios en campo del proveedor con el contratista para asistir en la implementación de la USP del proveedor.

f. Proporcionar actualizaciones regulares del estado del proyecto al contratista en relación a la implementación de las soluciones personalizadas (si corresponde) y la implementación de la USP del proveedor.

C. Servicio de Arquitecto de Soluciones:

1. El servicio de Arquitecto de Soluciones del proveedor deberá incluir un ingeniero de arquitectura de soluciones que actúe como único punto de contacto técnico durante la implementación de la USP y que será responsable de lo siguiente:

a. Asistir al contratista/subcontratista con el diseño y la arquitectura de la USP del proveedor.

b. Llevar a cabo actividades de consulta técnica que podrían incluir análisis de deficiencias/ajustes, revisiones de diseño del sistema, evaluaciones de compatibilidad de dispositivos, revisiones de diseño funcional y técnico, así como revisiones de rendimiento de la USP del proveedor.

c. Realizar una evaluación del sistema y garantizar el cumplimiento de las mejores prácticas de la USP del proveedor.

d. Proporcionar una estrategia de migración y actualización para la USP del proveedor según corresponda.

e. Proporcionar documentación con relación a la arquitectura del sistema, el diseño del sistema, las especificaciones de hardware y los requisitos de compatibilidad, los cálculos del ancho de banda de las cámaras y las mejores prácticas con respecto a la USP del proveedor.

D. Servicio de Configuración y Puesta en Marcha de Sistemas:

1. La Configuración del Sistema y el Servicio de Puerta en Marcha del proveedor deberá incluir un Ingeniero de Campo quien será responsable por:

a. Asistir a los técnicos en el lugar/remotos del contratista o subcontratista con la configuración y puesta en marcha de la USP del proveedor en el sitio del cliente.

b. Llevar a cabo una prueba de la USP después de la instalación del sistema usando escenarios del operador reales para asegurar un desempeño óptimo del sistema.

c. Proporcionar al contratista con un Informe de Servicio que indique con detalle las tareas realizadas durante la integración de la USP en el sitio del cliente, al igual que recomendaciones para mejorar el desempeño de la USP que deben ser implementadas por el contratista.

d. Proporcionar una transferencia de conocimiento de la USP del proveedor al contratista después de la implementación de la USP en el sitio del cliente.

3.03 Capacitación del Fabricante para el Operador Usuario Final *(Especificador: Este es un cargo de medio día más gastos)*

A. El contratista deberá contratar los servicios del proveedor de la USP para asistir en la capacitación del usuario final de la USP en el sitio final del usuario.

Genetec, Omnicast, Synergis, Federation, Sipelia, el logotipo Genetec y el logotipo Mobius Strip, son marcas registradas de Genetec Inc., y pueden estar registradas o tener el registro en trámite en varias jurisdicciones. El resto de las marcas comerciales utilizadas en este documento pueden ser marcas comerciales de los fabricantes o proveedores de los respectivos productos.

Sección 28 23 00 - Sistema de Administración de Video

Parte 1 - Información General

1.01 Trabajo relacionado

A. División 14 - Requisitos Generales para Elevadores

B. Sección 28 13 00 – Sistema Electrónico de Control de Acceso

1.02 Definiciones

A. ACS - Sistema de Control de Acceso

B. CSA - Aplicación de Software del Cliente

C. DGM - Mapas Gráficos Dinámicos

D. DVS - Servidor Digital de Video

E. ALPR – Reconocimiento Automático de Placas de Matrícula

F. SDK - Kit de Desarrollo de Software

G. GLM – Administración del Ciclo de Vida de Genetec

H. SSM - Módulo de Software del Servidor

I. UI - Interfaz de Usuario

J. USP - Plataforma Unificada de Seguridad

K. USW - Cliente Web Unificado

L. VMS - Sistema de Administración de Videos

1.03 Requisitos

A. El programador del sistema deberá haber asistido a la capacitación del fabricante y obtenido la Certificación Técnica en Security Center - Omnicast™ de Genetec™.

B. Como opción, el programador del sistema deberá haber asistido a la capacitación del fabricante y obtenido la Certificación Técnica en Security Center - Enterprise de Genetec.

C. El programador del sistema deberá ser un Socio de Negocios Certificado Genetec con el siguiente nivel de preparación: *(Especificador: seleccione una de las siguientes opciones)*

1. Socio de Negocios Certificado o superior
2. Socio de Negocios Élite o superior
3. Socio de Negocios Élite Unificado

D. El programador del sistema deberá presentar comprobante de las certificaciones.

Parte 2 - Productos

2.01 Requisitos generales del VMS

A. El VMS admitirá la actualización de los controladores de su cámara independientemente de la instalación del VMS. Se lanzarán controladores nuevos varias veces al año para ampliar la compatibilidad con nuevos dispositivos y funciones.

B. El VMS deberá basarse sobre una verdadera arquitectura abierta que deberá permitir el uso de estaciones de trabajo y hardware de servidores sin derechos de propiedad intelectual, infraestructura de red sin derechos de propiedad intelectual, y almacenamiento sin derechos de propiedad intelectual.

C. El VMS deberá ofrecer una solución completa y escalable de videovigilancia que deberá permitir la adición de cámaras sobre bases unitarias.

D. El VMS deberá interconectarse con codificadores de video análogos a digital y cámaras IP y con decodificadores de video digital a análogos, en lo sucesivo denominados como servidores de video digital (DVS). El VMS deberá soportar los DVS de varios fabricantes.

E. El VMS deberá integrar los DVS usando el SDK nativo de los DVS o usando la siguiente norma industrial para la conexión al DVS:

1. ONVIF

F. Todas las transmisiones de video suministradas desde cámaras analógicas o cámaras IP deberán estar codificadas digitalmente en formatos de compresión H.265, H.264, MPEG-4, MPEG-2, MJPEG, MxPEG, Wavelet o JPEG2000, y grabadas de manera simultánea en tiempo real.

G. Todos los flujos de audio suministrados desde servidores de video IP deberán estar codificadas digitalmente en formatos de compresión g711 (u-law), g721, g723, o AAC y grabadas simultáneamente en tiempo real.

H. La tasa de bits, la tasa de cuadros y la resolución deberán configurarse de manera independiente desde otras cámaras en el sistema, la modificación de estas configuraciones no deberá afectar las configuraciones de grabación y visualización de otras cámaras.

I. El VMS deberá ser capaz de usar múltiples teclados CCTV para el funcionamiento de todo el conjunto de cámaras del sistema, incluyendo marcas de cámaras de fabricantes diversos e incluyendo sus funcionalidades PTZ (por ejemplo, teclado Pelco controla domo Panasonic o viceversa).

J. El VMS deberá ser capaz de recuperar y fijar la posición actual de cámaras PTZ usando coordenadas XYZ.

K. El VMS deberá soportar los protocolos de cámara PTZ de múltiples fabricantes, incluyendo protocolos IP y análogos.

L. El VMS deberá arbitrar el conflicto del usuario sobre el uso de PTZ con base en los niveles de usuario por cámara.

M. El VMS deberá admitir la siguiente lista de teclados CCTV:

1. American Dynamics 2078 ASCII y American Dynamics 2088 ASCII
2. Bosch Autodome, Bosch Intuikey
3. DVTel
4. GE ImpactNet
5. Panasonic, Pelco ASCII, Pelco KBD-300, Pelco 9760 y Pelco P.
6. Radionica
7. Hanwha Techwin SSC-100, SPC-600, SPC-2010, SPC-6000 y SPC-7000.
8. Alarma de video
9. Sony RM-NS1000
10. Panasonic WV-CU161C
11. Teclado Ethernet Panasonic WV-CU950

N. El VMS deberá admitir la siguiente lista de controles de mando:

1. Eje 295
2. Tablero de control de videovigilancia Axis T8310, T8311, T8312, T8313
3. Cualquier control de mando USB detectado como un controlador de juegos de Windows

O. El VMS deberá soportar el cambio de contraseña para la siguiente lista de unidades de video:

1. Series H3 y H4 de Aviglion.
2. Axis: Todas las unidades con el firmware 6.50 o versiones posteriores.
3. Bosch: Todas las unidades con el firmware 6.30 o versiones posteriores.
4. Hanwha: Las siguientes series son compatibles:
    a. Toda la serie X (todas las versiones de firmware)
    b. Toda la serie PNx (las versiones de firmware 1.01 y posteriores)
    c. Todos los SPE-xx10 (todas las versiones de firmware), excepto SPE-100, SPE-400, SPE-101
    d. Toda la serie Q (todas las versiones de firmware), excepto QNO-6010R, QNO-6020R, QNO-6030R, QND-6010R, QND-6020R, QND-6030R, QNV-6010R, QNV-6020R, QNV-6030R, QNE-6080RV, QNE-7080RV
    e. Toda la serie L (todas las versiones de firmware)

f. Toda la serie TNx (todas las versiones de firmware) excepto TNU-6320

5. ONVIF: Compatible con el perfil S.

6. Panasonic: Todas las unidades y todos los firmwares.

P. El VMS deberá permitir la configuración de un huso horario para cada cámara conectada a un DVS. Para revisar la reproducción, los usuarios tendrán la habilidad de buscar los videos en base a las siguientes opciones:

1. Hora local de la cámara

2. Hora local del SSM

3. Hora local de la estación de trabajo del usuario

4. Hora GMT

5. Otros husos horarios

Q. La configuración del almacenamiento de audio y video para el SSM deberá ser:

1. IDE/SATA/SAS internos y externos organizados o no en una configuración RAID.

2. Interno o externo SCSI/iSCSI/Fiber Channel organizados o no en una configuración RAID.

3. Dentro del sistema global de almacenamiento, será posible incluir discos ubicados en:

a. PC externas en una LAN o WAN

b. Servidores Adjuntos a Redes (NAS) en una LAN o WAN

c. Redes de Área de Almacenamiento (SAN)

R. El SSM no deberá limitar la capacidad de almacenamiento actual configurada por servidor.

S. Fabricante:

1. Genetec Security Center: *(Especificador: seleccione una de las siguientes opciones)*

a. Omnicast Enterprise

b. Omnicast Professional

c. Omnicast Standard

2.02 Requisitos de seguridad cibernética

A. La USP deberá ser una solución habilitada para IP. Toda la comunicación entre el SSM y la CSA estará basada en el protocolo TCP/IP estándar y deberá usar la encriptación TLS con certificados digitales para proteger el canal de comunicación.

B. La USP deberá soportar la autenticación de usuario con autenticación basada en notificaciones usando proveedores externos. Los proveedores externos deberán incluir:

   1. ADFS (Servicios de federación de Active Directory)
   2. Azure Active Directory (a través de OpenID Connect)
   3. Ping Identity (a través de OpenID Connect)
   4. KeyCloak (a través de OpenID Connect)
   5. Otros agentes de autenticación de Open ID Connect/SAML2

C. La USP deberá limitar los puertos IP en uso y deberá proporcionar al Administrador la habilidad de configurar estos puertos.

D. El VMS deberá soportar solo peticiones seguras de flujos de medios, a menos que esté configurada explícitamente de otra forma. Las peticiones seguras de flujos de medios deberán estar protegidas con autenticación sólida basada en certificados aprovechando RTSPS (RTSP sobre TLS). La autenticación del cliente para las peticiones de flujos de medios está basada en notificaciones y puede usar un token de seguridad de duración limitada.

E. El VMS deberá ofrecer la habilidad de encriptar los flujos de medios, incluyendo video, audio y metadatos con encriptación autenticada. La encriptación de flujos de medios deberá hacerse en reposo y en tránsito y puede ser una encriptación certificada en base a AES de 128 bits. El VMS deberá:

   1. Permitir la encriptación a establecerse por cámara para todas o algunas de las cámaras.
   2. Proporcionar hasta 20 certificados diferentes para diferentes grupos de CSA o usuarios que les han recibido acceso a flujos no encriptados.
   3. No reducir el rendimiento de grabación en más del 50% cuando la encriptación está habilitada.
   4. Usar RTP Seguro (SRTP) para el encriptado de carga útil de un flujo de medios en tránsito y permitir la multidifusión y unidifusión de las secuencias encriptadas.
   5. Utilizar una clave de encriptación al azar y cambiarla periódicamente.
   6. Permitir la exportación de flujos encriptados.

F. El VMS deberá soportar los flujos encriptados de punto a punto con cámaras que soporten RTP seguro (SRTP) tanto en unidifusiones y multidifusiones desde la cámara.

G. La USP deberá soportar encriptación de todas las comunicaciones y sus bases de datos.

H. En la interfaz de usuario principal, la USP deberá proporcionar una lista visual del estado de todos los elementos de configuración relacionados con el nivel de seguridad cibernética de las funciones del sistema.

I. La USP deberá proporcionar recomendaciones relacionadas con las contraseñas utilizadas para acceder a las unidades de hardware del sistema. En las recomendaciones, se deberá indicar si las contraseñas utilizadas en las unidades son débiles, intermedias, robustas o muy robustas.

J. La USP deberá proporcionar la habilidad de cambiar las contraseñas de la unidad de video, de manera manual o automática, con la API nativa del fabricante, el Genetec Protocol estándar u ONVIF. El VMS deberá soportar el cambio de contraseña de las unidades de video de la siguiente manera:

1. En lote o por unidad
2. En la fecha prevista
3. Desde un evento
4. Según las políticas del fabricante
5. La USP deberá permitir realizar una copia de respaldo de las últimas cinco contraseñas.
6. La USP deberá permitir copiar la contraseña al portapapeles para usarla en la página web del dispositivo si el usuario tiene los privilegios apropiados.
7. La USP deberá proporcionar la habilidad de exportar las contraseñas de la unidad de video si el usuario tiene los privilegios apropiados.

K. La USP deberá proporcionar recomendaciones relacionadas con el firmware de las unidades de hardware registradas en el sistema. En las recomendaciones, se deberá indicar si el firmware está actualizado o desactualizado, y si posee vulnerabilidades de seguridad conocidas.

2.03 Requisitos de conmutación por error y espera

A. La USP deberá soportar opciones de conmutación por error nativas y las que se adquieren libremente en el mercado.

B. Directory de Conmutación por Error: *(Especificador, se requiere licencia adicional por cada servidor que conmutará, solo Enterprise)*

1. El Directory en Modo de Espera deberá actuar como un SSM de reemplazo en estado de espera rápida, listo para actuar como el Directory actual en caso de falla del Directory principal. La conmutación por error deberá presentarse en menos de un minuto. No será necesaria ninguna acción por parte del usuario.
2. La USP deberá soportar hasta cinco (5) Directories en modo de espera, alineados para actuar como el Directory actual en una forma de cascada.
3. El Directory en Modo de Espera deberá conservar su base de datos de configuración sincronizada con el Directory principal.
4. El Directory en Modo de Espera deberá soportar escenarios de recuperación ante desastres en donde un servidor puede estar ubicado en otra área geográfica (o edificio) y encargase solamente si todos los otros directorios pasan a estar fuera de línea.

5. El Directory en Modo de Espera deberá soportar la sincronización de las bases de datos de configuración usando un mecanismo de copia de seguridad y restauración. El período de sincronización se podrá configurar desde 15 minutos hasta una semana.

6. El Directory en Modo de Espera deberá soportar la sincronización en tiempo real de las bases de datos de configuración que usan SQL Mirroring o SQL Always On.

C. Archiver En Espera Consulte la sección 2.05 Archiver en Espera para mayor información.

D. Las opciones de modo de espera/conmutación por error adquiridas de forma libre en el mercado (sin incluir el Archiver del VMS) deberán incluir: *(Especificador: se requiere licencia adicional por servidor que conmutará por error; solo Enterprise)*

1. Clústeres de Windows

2. NEC ExpressCluster X LAN

2.04 Archivado

A. El Archiver (función) deberá usar un evento y base de datos de marca de tiempo para la búsqueda avanzada de archivos de audio/video. Esta base de datos deberá usar Microsoft SQL.

B. El Archiver deberá proteger los archivos de audio/video archivados y la base de datos del sistema contra el acceso a la red y el acceso de usuarios no administrativos.

C. El Archiver filmará digitalmente el video grabado usando un algoritmo de firma EdDSA basado en una clave criptográfica pública/privada.

D. El Archiver deberá ofrecer un servicio de descubrimiento de hardware del tipo plug and play con las siguientes funcionalidades:

1. Detección automática de unidades DVS adjuntas a la red.

2. Detectar unidades DVS sobre diferentes segmentos de red, incluyendo la Internet y a lo largo de enrutadores con o sin capacidades de conversión de direcciones de red (NAT).

E. El Archiver tendrá la capacidad de configurar el intervalo de cuadro clave (I-frame) en segundos o números de fotogramas.

F. El Archiver deberá proporcionar una opción de grabación antes y después de la alarma que se pueda configurar entre un segundo y 5 minutos por cámara.

G. El Archiver deberá proporcionar la funcionalidad de almacenar flujos de video y audio con base a eventos desencadenantes, como:

1. Detección de movimientos digital

2. Activación de entrada digital

3. Macros
4. Mediante la grabación de la aplicación del SDK

H. El Archiver deberá realizar la detección de movimiento de video en cada cámara individual con base a una cuadricula de 1320 bloques de detección de movimiento. Todas las configuraciones de detección de movimiento de video son configurables en un cronograma. Se cuenta con un umbral global de sensibilidad para reducir la sensibilidad de la detección de movimiento cuando la señal de video tiene mucho ruido o cuando se han incurrido en muchos aciertos falsos. La detección de movimiento de video en sí se puede establecer en cuatro modos diferentes:

1. Pantalla completa: Se activan todos los 1320 bloques en la pantalla, y se puede configurar un umbral general para el movimiento global en toda la imagen, y cuando se alcanza, puede activar la grabación de un evento de movimiento o un evento personalizado.
2. Unidad de Pantalla Completa: Esto es lo mismo que la Pantalla Completa pero la detección de movimiento se lleva a cabo en los DVS.
3. Zona de Detección: Se podrán definir seis zonas superpuestas en los 1320 bloques en la pantalla con cada una de las zonas con su propio umbral, y, al alcanzarse el umbral, cada una de ellas puede activar la grabación de un evento de movimiento o un evento personalizado. Cada zona que activa su propio evento permite la configuración de los eventos de detección de movimiento direccionales y otra lógica de detección de movimiento compleja.
4. Unidad de Zona de Detección: Esto es lo mismo que la Zona de Detección, pero la detección de movimiento se lleva a cabo en el DVS y solo se soporta una zona.
5. Deshabilitado: No se realiza ninguna detección de movimiento en esta cámara.

I. El Archiver deberá ser capaz de detectar movimiento en video dentro de 200 milisegundos y no solo en los fotogramas clave.

J. El Archiver deberá permitir que se asignen múltiples cronogramas de grabación a una sola cámara. Cada cronograma deberá crearse con los siguientes parámetros:

1. Modo de grabación:
   a. Continuo
   b. En Movimiento/Manual
   c. Manual
   d. Desactivado
2. Patrón de periodicidad:
   a. Una vez en días específicos
   b. Días específicos con periodicidad anual
   c. Días específicos con periodicidad mensual

d. Días específicos con periodicidad semanal

e. A diario

K. Cobertura de tiempo:

a. Todo el día.

b. Rango(s) específico(s) de tiempo.

c. De día o de noche con base en las horas del amanecer y atardecer las cuales se calculan automáticamente a partir de la época del año y una ubicación geográfica. Se deberán ofrecer disposiciones para compensar el cálculo del amanecer o atardecer por más o menos de 3 horas.

L. El Archiver deberá permitir a cada cámara (fuente de video) codificarse múltiples veces de la misma forma o en diferentes formatos de video (H.265, H.264, MPEG-4, MPEG-2, MJPEG, MxPEG, Wavelet o JPEG2000), solo limitado por las capacidades de cada DVS.

M. Cuando se cuenta con varias transmisiones de video desde la misma cámara, los usuarios tendrán la libertad de usar cualquiera de ellas con base en su uso asignado. Los usos de transmisión de video estándar son:

1. En vivo
2. Grabación
3. Remoto
4. Baja resolución
5. Alta resolución

N. El Archiver deberá permitir que la calidad de video varíe de acuerdo a los cronogramas predefinidos. Dichos cronogramas deberán contar con la misma flexibilidad de configuración que los cronogramas de grabación mencionados con anterioridad. La calidad de video deberá basarse en, más no limitarse a, los siguientes parámetros:

1. Tasa de bits máxima
2. Máximo índice de cuadros
3. Calidad de imagen
4. Intervalos de cuadros clave

O. El Archiver deberá contar con la habilidad de impulsar de forma dinámica la calidad del ‘flujo de grabación’ (ver viñeta anterior) con base en eventos específicos:

1. Cuando la grabación se inicia manualmente por un usuario.
2. Cuando la grabación se activa por un macro, una alarma o la detección de un movimiento.

P. El Archiver deberá tener la capacidad de comunicarse con el DVS usando encriptación SSL de 128 bits.

Q. El Archiver tendrá la capacidad de comunicarse con el DVS usando el protocolo seguro HTTPS.

R. El Archiver tendrá la capacidad de recibir flujos UDP de multidifusión directamente desde el DVS.

S. Para topologías de red que restringen al DVS para enviar flujos UDP de multidifusión, el Archiver deberá redirigir las transmisiones de audio/video a clientes visualizando de manera activa en la red usando UDP de multidifusión.

T. El Archiver deberá tener la capacidad para redirigir las transmisiones de audio/video a clientes de visualización activa en la red usando la UDP o TCP de unidifusión.

U. El Archiver deberá facultar al administrador con un amplio rango de opciones de administración de disco:

1. El Archiver deberá permitir al administrador elegir cuáles discos usar para el archivamiento y para establecer una máxima cuota para cada uno.
2. El Archiver deberá permitir al administrador esparcir el archivado de diferentes cámaras sobre diferentes grupos de disco (grupos de disco controlados por el mismo controlador) de manera que el archivamiento pueda llevarse a cabo en paralelo sobre discos múltiples.
3. El Archiver deberá tener la capacidad de mover archivos de video a la Nube Azure. Los archivos se moverán después de un número preestablecido de días.

V. El Archiver facultará al administrador con un amplio rango de opciones de administración de archivo:

1. El Archiver deberá proporcionar una representación gráfica de secuencias de videos y las brechas en la grabación.
2. El Archiver deberá proporcionar una forma de identificar la ubicación de las secuencias de videos.

W. El Archiver deberá ofrecer las siguientes opciones para limpiar archivos antiguos, en una cámara y en base a una cámara:

1. Después de un número preestablecido de días.
2. Eliminar archivos más antiguos primero cuando se acaba el espacio del disco.
3. Detener el archivado cuando los discos están llenos.

X. El Archiver deberá permitir que se protejan secuencias importantes de videos contra las limpiezas rutinarias de los discos.

Y. Los usuarios deberán tener las siguientes opciones al proteger una secuencia de video:

1. Hasta una fecha específica

2. Por una cantidad específica de días
3. Indefinidamente (hasta que la protección se elimine explícitamente)

Z. El Archiver deberá permitir al administrador colocar un porcentaje tope para el espacio de almacenamiento ocupado por videos protegidos.

AA. El Archiver deberá mantener un registro y compilar estadísticas sobre el uso de espacio del disco.

1. Las estadísticas estarán disponibles por grupo de disco o para todo el Archiver.
2. Las estadísticas deberán mostrar el porcentaje de videos protegido sobre el espacio total del disco usado.

BB. El Archiver deberá tener la capacidad de disminuir la tasas de transmisión de videos con el propósito de ahorrar almacenamiento. Las opciones de disminución de las tasas disponibles son las siguientes:

1. Las opciones para la disminución de tasas de flujos H.264, MPEG-4, y H.265, son: todos los cuadros clave, 1 fps, 2 seg./cuadro, 5 seg./cuadro, 10 seg./cuadro, 15 seg./cuadro, 30 seg./cuadro, 60 seg/cuadro, 120 seg./cuadro.
2. Para flujos MJPEG las opciones de disminución de las tasas son: 15 fps, 10 fps, 5 fps, 2 fps, 1 fps, 2 seg./cuadro, 5 seg/cuadro, 10 seg/cuadro, 15 seg/cuadro, 30 seg/cuadro, 60 seg/cuadro, 120 seg/cuadro.

CC. El Archiver deberá soportar DVS con capacidades de grabación en la periferia y ofrecer la siguiente capacidad:

1. La habilidad de reproducir video grabado en el DVS a diferentes velocidades.
2. La habilidad de descargar (grabación selectiva de videos) video grabado en el DVS en el horario estipulado, cuando sucede un evento, o de manera manual para almacenarlo en el Archiver.
3. Deberá ser posible filtrar el video que se está descargando usando uno o varios de los siguientes filtros:
    a. Intervalo de tiempo
    b. Solicitudes de reproducción
    c. Eventos de analíticas de video
    d. Eventos de movimiento
    e. Marcadores
    f. Alarmas
    g. Eventos de clavijas de entrada
    h. Eventos fuera de línea de la unidad

DD. El Archiver deberá recibir datos de desempeño y escalabilidad comprobados:

1. El desempeño del Archiver deberá ser garantizado durante la reconstrucción de un disco desde un grupo de disco raid 5. El proceso de reconstrucción no deberá afectar las capacidades de grabación y reproducción.
2. La especificación de servidores recomendados del Requisito de Hardware de Security Center de Genetec deberá permitir al Archiver actuar hasta 300 cámaras o cuando se alcance el primer límite rendimiento de 300 MB.
3. La especificación de Archiver de alto rendimiento correspondiente al Requisito de Hardware de Genetec Security Center deberá permitir que el Archiver haga lo siguiente: *(Especificador, para máquinas preseleccionadas)*
    a. Un rendimiento de hasta 500 cámaras o 500Mbs de primer limite alcanzado con un NIC de 1Gbps.
    b. Un rendimiento de hasta 700 cámaras o 1300Mbs de primer limite alcanzado con un NIC de 10Gbps.

EE. El Archiver deberá proporcionar la capacidad de encriptar la transmisión de medios que provienen del DVS, lo que incluye el video, el audio y los metadatos: *(Especificador, solo Enterprise, se requiere licencia adicional)*

1. La encriptación de medios deberá ser opcional y se podrá activar con base a DVS.
2. La encriptación de medios deberá realizarse con AES-128 bits.
3. La encriptación de medios deberá encriptar todo el video, audio y metadatos en reposo y en tránsito. Una vez que se encienda la encriptación de medios para un DVS todos los medios almacenados o redirigidos por el Archiver deberán encriptarse y deberán requerir una clave privada para descodificarlo.
4. Deberá ser posible exportar los medios encriptados en un archivo ASF sin encriptar.

2.05 Auxiliary Archiver *(Especificador: se requiere licencia adicional; solo Enterprise)*

A. El Auxiliary Archiver será usado para producir archivos redundantes (video, eventos o marcadores) de cualquier cámara en el sistema, en base a caso por caso.

B. El Auxiliary Archiver deberá contar con la habilidad de grabar una cámara en un cronograma diferente al del Archiver.

C. El Auxiliary Archiver deberá contar con la habilidad de archivar cualquiera de las transmisiones de video estándar para el archivamiento. Los usos de transmisión de video estándar son: En Vivo, Grabando, Remoto, Baja Resolución y Alta Resolución.

D. El Auxiliary Archiver deberá tener la capacidad de mover archivos de video a la Nube Azure.

2.06 Standby Archiver *(Especificador: solo Enterprise, requiere una licencia adicional por DVS que conmutará por error)*

A. El Standby Archiver deberá actuar como una función de Archiver de reemplazo en estado de espera activa, listo para encargarse de las funciones de la función

principal del Archiver. La conmutación por error deberá presentarse en menos de 1 minuto. No será necesaria ninguna acción por parte del usuario.

B. El Standby Archiver asignado a una entidad de función de Archiver deberá ofrecer de forma automática protección para todo el DVS que está conectado a dicha función de Archiver.

C. El Standby Archiver deberá proteger la función principal del Archiver contra las siguientes fallas:

1. Falla del servidor (hardware o software).

2. Falla de almacenamiento, como cuando la Función de Archiver detecta que no puede leer o escribir a ninguno de sus discos asignados.

D. Deberá ser posible que un solo servidor de la USP actúe como el servidor en espera de varias funciones del Archiver.

1. Cada función de Archiver deberá contar con un valor de prioridad si varias Funciones de Archiver fallan a la misma vez en el mismo servidor en espera.

E. Deberá ser posible que cualquier función del Archiver en el sistema se designe como el modo de espera de otro y viceversa.

F. Para cada función de Archiver será posible establecer hasta 2 Archiver en espera de manera que si falla la primera conmutación por error del Archiver, la conmutación ocurrirá de forma automática a un tercer servidor.

G. El Standby Archiver deberá contar con la habilidad de actuar como un Redundant Archiver.

H. Deberá ser posible establecer un período de retención diferente para el Archiver y el Redundant Archiver .

I. El Redundant Archiver deberá mantener una copia exacta de todo lo grabado por el Archiver predeterminado, es decir, archivos de audio/video, eventos y marcadores.

J. La redundancia deberá configurarse de cámara en cámara.

K. El Redundant Archiver tendrá la habilidad de usar una transmisión de video de multidifusión desde el DVS y no deberá requerir una conexión adicional a ningún DVS.

2.07 Archivado de nube

A. El VMS deberá soportar la transferencia automática de videos grabados en el Archiver a la nube, con base en la edad del video.

B. El Archiver cifrará las grabaciones usando AES-256 antes de transferir el video a la nube.

C. El Archiver rotará la clave de cifrado en cada archivo. La clave de cifrado se cifrará con un certificado guardado en Azure Key Vault.

D. El VMS deberá soportar la encriptación TLS entre el Archiver de las instalaciones y la nube.

E. El VMS deberá permitir a los usuarios buscar video almacenado en la nube mediante la misma funcionalidad cuando se consulta video que se almacenó de forma local.

F. El VMS deberá mantener un caché local de video descargado desde la nube, con el objetivo de reproducir grabaciones sin la necesidad de una transferencia adicional.

G. El VMS admitirá diferentes niveles para admitir las secuencias de videos.

1. El VSM permitirá a los usuarios diferenciar las secuencias de videos disponibles para recuperación en tiempo real y con retraso.

2. El VMS moverá de manera automática las secuencias de videos del acceso en tiempo real a la recuperación con retraso después de un retraso configurable.

2.08 Transmisión de video del VMS

A. La Función del Media Router será responsable de enrutar los flujos de video y audio en redes locales y de área extensa, desde la fuente (como el DVS) hacia el destino (como la CSA).

B. La Función del Media Router deberá soportar múltiples protocolos de transporte, como lo son TCP de unidifusión, UDP de unidifusión y UDP de multidifusión.

C. El Media Router deberá soportar IGMP (Protocolo de Administración de Grupos de Internet) para establecer membresías de grupos de multidifusión:

1. Se deberá soportar IGMP v3, incluyendo SSM (Multidifusión Específica a la Fuente).

D. La Función del Media Router usando Agentes Redirectores deberá ser responsable por redirigir un flujo desde un extremo IP de la fuente a un extremo IP del destino.

E. Los Agentes Redirectores serán capaces de convertir un flujo desde y hacia cualquier protocolo de transporte soportado:

1. UDP de Multidifusión a TCP de Unidifusión

2. UDP de Multidifusión a UDP de Unidifusión

3. TCP de Unidifusión a UDP de Multidifusión

4. UDP de Unidifusión a UDP de Multidifusión

F. Será posible limitar el número de redirecciones en vivo concurrentes y reproducciones de video para cada Agente Redirector a manera de controlar mejor el ancho de banda lo largo de múltiples sitios.

G. Deberá ser posible limitar el ancho de banda consumido por videos en vivo y reproducciones desde el CSA para controlar mejor el ancho de banda entre varios sitios. El SSM deberá ser capaz de dar prioridad a la transmisión de video al CSA con base en el nivel de usuario.

H. Será posible proteger la función del Media Router contra la falta de disponibilidad de hardware o software al configurar otra Función del Media Router para actuar como un servidor en espera activa.

I. Se deberá usar varios Agentes Redirectores en una instalación VMS grande para aumentar la disponibilidad de servicio y para proporcionar equilibrado de carga automático.

2.09 Capacidades de transferencia de archivos de video del VMS

A. La transferencia de archivos deberá proporcionar la habilidad de:

1. Transferir video desde un servidor a otro servidor en el mismo sistema.
2. Transferir video desde un servidor federado a otro servidor.
3. Transferir video desde un almacenamiento de cámara a otro servidor.

B. Será posible programar transferencias de videos tanto en un cronograma recurrente, como accionarlas de forma manual o al momento de la conexión.

C. Será posible filtrar el video de interés para una transferencia. El video de interés estará definido con los siguientes filtros:

1. Todos los archivos cuando la cámara estaba fuera de línea.
2. Alarmas.
3. Petición de reproducción desde la periferia.
4. Eventos de analíticas de videos.
5. Eventos de movimiento.
6. Marcadores.
7. Activadores de entradas.
8. Rango de tiempo.

D. Será posible definir la duración del video antes y después del evento cuando se usa como un filtro para determinar el video de interés.

E. La USP deberá ofrecer una interfaz para la visualización de todas las peticiones de transferencia de archivos de video. Esta interfaz deberá mostrar todas las solicitudes de transferencia actuales, solicitadas y programadas. Deberá ser posible editar, accionar y cancelar las transferencias de archivos de video desde esta interfaz.

F. La USP ofrecerá una interfaz para consultar transferencias de video pasadas y su resultado.

2.10 Video Analíticas de Seguridad

A. Las analíticas deben unificarse por completo con el Sistema de Administración de Videos.

B. La configuración deberá realizarse de forma nativa en la interfaz de configuración del Sistema de Administración de Videos.

C. Las analíticas deberán contar con posibles configuraciones para los siguientes escenarios:

   1. Protección de perímetros
   2. Protección de áreas
   3. Control de dirección
   4. Detección de objetos
   5. Detección de vehículos detenidos
   6. Detección de Entrada Sin Autorización al Seguir de Cerca

D. Cada escenario podrá activar eventos en el Sistema de Administración de Videos que correspondan a su funcionalidad.

E. Además de estos escenarios, las analíticas deberán permitir la configuración de escenarios personalizados para la detección de intrusiones y objetos, y facilitar la importación de ajustes para ofrecer la máxima flexibilidad.

F. La licencia de las analíticas deberá permitir la configuración de cualquiera de estos escenarios por cámara.

G. Las analíticas deben permitir, como mínimo, dos variantes de detección:

   a. Activar una alarma si un patrón de movimiento se mueve de la zona A (fuente) a través de la zona B hasta la zona C (receptor).
   b. Activar una alarma si un patrón de movimiento se mueve en cualquier lugar dentro de una zona especificada.

H. Las analíticas deben soportar una cantidad ilimitada de áreas de detección.

I. Las analíticas deben contar con filtros de lluvia para filtrar las interrupciones.

J. Las analíticas deben contar con una configuración en vivo que permita ver de inmediato las consecuencias de un cambio de parámetro en la interfaz de configuración sin necesidad de guardar las nuevas configuraciones.

K. La configuración de las analíticas se podrá implementar en transmisiones de video grabadas.

L. Las analíticas deben ofrecer la posibilidad de configurar trayectorias de movimiento de objetos.

M. Las analíticas no deben emplear puntos de activación o líneas cruzadas.

N. Las áreas y la perspectiva de las escenas (tamaño del objeto cerca y lejos) deben configurarse en pantalla usando una interfaz de apuntar y hacer clic.

O. Las analíticas deben contar con filtros para la velocidad, distancia y dirección de los movimientos para detectar eventos.

P. Las analíticas deberán contar con opciones para mostrar u ocultar áreas, nombres de áreas y superposiciones de detección de forma independiente.

Q. Las analíticas deben estar basadas en servidores en su totalidad, sin necesitad de cálculos en cámaras.

R. Las analíticas deben funcionar con cámaras a color, térmicas e infrarrojas.

S. El Programa de Evaluación de Video Analíticas del CPNI deberá evaluar y aprobar la precisión de las analíticas, que se incluirá en el Catálogo de Equipos de Seguridad (CSE, por sus siglas en inglés) del CPNI.

2.11 Monitor de integridad de la cámara

A. Descripción:

1. Comprueba de manera automática las transmisiones de las cámaras para detectar si hubo alteraciones.

2. Se puede utilizar para alertar casi en tiempo real los eventos de alteración o se puede usar como una herramienta de mantenimiento.

3. Se pueden ejecutar informes sobre los eventos de alteración detectados.

B. Detalles:

1. Se deberá unificar de manera completa con el Sistema de Administración de Videos.

2. Deberá ser posible definir la sensibilidad de detección de las transmisiones de cada cámara: baja, media o alta.

3. Deberá ser posible elegir el servidor donde se ejecutarán las analíticas.

4. Deberá ser posible configurar la transmisión de la cámara utilizada para las analíticas.

5. Deberá ser posible definir la cantidad de cámaras que sea analizan al mismo tiempo.

6. Para utilizar la mínima cantidad de recursos, deberá ser posible definir la frecuencia de análisis de las transmisiones de las cámaras.

7. Deberá ser posible conocer las cámaras configuradas para análisis.

2.12 Protector de Privacidad

A. Descripción:

1. Oscurece todo el movimiento en videos de vigilancia en tiempo real, de forma automática.

2. Enmascaramiento de privacidad en vivo de objetos en movimiento (como personas y vehículos).
3. Completamente unificado con el sistema de administración de videos.
4. Configuración nativa en la interfaz de configuración del sistema de administración de videos.

B. Detalles:

1. Certificado con un sello de certificación EuroPriSe válido.
2. El enmascaramiento de privacidad se puede eliminar por cámara o para todas las cámaras que se ven actualmente. El enmascaramiento de todas las cámaras visualizadas se puede eliminar y agregar de manera manual con un botón o de manera automática con una acción.
3. Modos de interiores / exteriores que usan un modelado flexible de fondos:
    a. Interiores: Modelo de aprendizaje con hasta 10 estados de iluminación diferentes esto permite adaptarse a cambios de iluminación rápidos, como luces que se encienden y se apagan.
    b. Exteriores: Detección en primer plano sobre la base de detección periférica en lugar de por color esto permite adaptarse a condiciones de iluminación muy cambiantes, como nubes que bloquean de manera temporal la luz solar.
4. Detecta movimientos mediante el uso de una imagen de diferencia absoluta, que se calcula al restar el cuadro actual de un modelo de fondo calculado.
5. Enmascara movimientos con bloques y, por lo tanto, oscurece el contorno de un objeto o persona.
6. Hay tres métodos de cifrado diferentes: Pixelar, Teñir y Transparencia.
7. Las cuadrículas de enmascaramiento se pueden configurar en una interfaz de apuntar y hacer clic.
8. Se encuentra disponible el modo de vista previa histórica para ver los cambios de configuración en la interfaz de configuración sin necesidad de guardar la configuración.
9. Las zonas pueden ser polígonos definidos sin restricciones con una interfaz de apuntar y hacer clic.
10. Opción de configurar la resolución del análisis para optimizar el rendimiento.
11. No es necesario realizar un cálculo en la cámara, se basa por completo en servidores.
12. Se ofrece la opción de definir zonas que se deben pixelar en todo momento o en ningún momento.
13. Se ofrece la opción de elegir los parámetros de las secuencias de entrada y salida, incluyendo la resolución, la tasa de cuadros y la codificación.

14. Emplea aceleración por hardware en el extremo del servidor para maximizar la cantidad de cámaras analizadas por servidor.

2.13 Contador de personas

A. Descripción:

1. Cuenta de manera automática las personas en el campo de visión de una cámara.
2. Proporciona widgets de tablero de control en vivo dedicados al conteo de personas.
3. Completamente unificado en el sistema de administración de videos.
4. Configuración nativa en la interfaz de configuración del sistema de administración de videos.

B. Detalles:

1. Basado en modelos de aprendizaje profundo capacitados en detección de personas para excluir objetos no humanos.
2. Widgets de tablero de control destinados al conteo de personas con las siguientes características:
    a. Gráficos: visualización de recuentos en gráficos de líneas o de barras
    b. Tráfico: Muestra la cantidad de personas en un marco de tiempo determinado.
    c. Ocupación: Muestra cuántas personas hay en un área (el conteo de entrada menos el conteo de salida)
3. Cuenta los adultos y los niños.
4. Cuenta las personas en sillas de ruedas.
5. Admite vistas de cámara de techo.
6. Admite el conteo bidireccional.
7. Admite vistas de cámara inclinada.
8. Opción para mostrar/ocultar superposiciones con las personas detectadas y la línea de conteo.
9. No se requiere una GPU para ejecutarse.
10. El widget de ocupación admite el restablecimiento del recuento en una opción de tiempo definido para definir zonas, que siempre o nunca deben pixelarse.
11. Admite la organización de cámaras en áreas y muestra estas áreas en widgets.
12. Emplea aceleración por hardware en el extremo del servidor para maximizar la cantidad de cámaras analizadas por servidor.

13. Los recuentos se pueden integrar a sistemas externos utilizando exportaciones CSV y un SDK de .NET

2.14 Requisitos Generales de Software de Clientes

A. Las Aplicaciones de Software de Cliente (CSA, por sus siglas en inglés) deberán proporcionar la interfaz de usuario para la configuración USP y el monitoreo sobre cualquier red, y estar accesibles de manera local o desde una conexión remota.

B. Las CSA deberán de consistir de la UI de Configuración para la configuración del sistema y el monitoreo de la UI de Monitoreo. Las CSA deberán tener una base Windows y proporcionar una interfaz de usuario (UI) gráfica fácil de usar.

C. Las CSA para monitoreo deberán soportar el funcionamiento en modo de 64 bits.

D. Se deberá usar el Server Administrator para configurar la(s) base(s) de datos del servidor. Deberá estar basado en la Web y ser accesible de forma local en el SSM o a lo largo de la red.

E. Las CSA deberán fusionarse de manera transparente con el control de acceso, el reconocimiento de placas de matrícula (ALPR, por sus siglas en inglés), y las funcionalidades de video dentro de la misma aplicación de usuario.

F. La USP deberá usar el desarrollo y las tecnologías de programación más recientes de interfaz de usuario (UI) como lo son Microsoft WPF (Windows Presentation Foundation), el lenguaje de marcado XAML, y la plataforma del software .NET.

G. Todas las aplicaciones deberán proporcionar un mecanismo de autenticación, el cual verifica la validez del usuario. Como tal, el administrador (quien cuenta con todos los derechos y privilegios) puede definir derechos y privilegios de acceso específicos para cada usuario en el sistema.

H. Se iniciará sesión en una CSA a través de cuentas y contraseñas de la USP almacenadas de manera local o a través de las credenciales del operador de Windows cuando esté habilitada la integración del Active Directory. *(Especificador: Professional y versiones superiores; se requiere licencia para Active Directory)*

I. Cuando está integrado con el Active Directory de Microsoft, la CSA y la USP deberán autenticar a los usuarios usando las credenciales de Windows. Como resultado de esto, la USP se beneficiará de la autenticación de contraseña y las poderosas características de seguridad del Active Directory. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

J. Cuando se integra con un proveedor de identidad externo como Windows Active Directory, ADFS (Active Directory Federation Services) o un proveedor de identidad de Open ID Connect/SAML2 (p. ej., Azure AD), la CSA y la USP deberán autenticar a los usuarios mediante una experiencia de Inicio de Sesión Única. Como resultado, la USP se beneficiará de volver a usar la misma credencial en todas las aplicaciones empresariales. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

K. La CSA deberá soportar múltiples idiomas, lo que incluye, entre otros, los siguientes: inglés, francés, árabe, checo, holandés, alemán, hebreo, húngaro, italiano, japonés,

coreano, noruego, persa (farsi), polaco, portugués (Brasil), chino simplificado y tradicional, ruso, español, sueco, tailandés, turco y vietnamita.

L. Para mejorar la usabilidad y la eficiencia del operador, la UI de Configuración y la UI de Monitoreo deberán soportar muchas de las más recientes UI, como:

1. Una Página de Inicio personalizable que incluya tareas favoritas y usadas recientemente.
2. Un enfoque orientado a tareas para las actividades del administrador/operador en donde cada tipo de actividad (vigilancia, administración de visitantes, informes individuales, y otros) es una tarea del operador.
3. Flujos de trabajo consolidados y consistentes para videos, ALPR y control de acceso.
4. Funcionalidad con un solo clic para generación de informes y rastreo. La UI de Monitoreo deberá soportar tanto la generación de informes para el control de acceso, ALPR y videos con un solo clic, así como el rastreo de áreas, cámaras, puertas, zonas, tarjetahabientes, elevadores, entidades ALPR, y otras con un solo clic. La generación de informes o rastreos con un solo clic deberá crear una nueva tarea con las entidades seleccionadas a reportar o rastrear.

M. Página de Inicio y Tareas de la UI de Configuración y la UI de Monitoreo.

1. La UI de Configuración y la UI de Monitoreo deberán estar orientadas a tareas.
2. Una tarea deberá ser patrones de diseño de interfaz de usuario cuyo objetivo sea simplificar la interfaz de usuario mediante la agrupación de características similares desde diferentes sistemas, como video y acceso, en la misma ventana de visualización. Las características deberán agruparse juntas en una tarea con base en su habilidad compartida para ayudar al usuario a realizar una tarea específica.
3. Se tendrá acceso a las tareas a través de la Página de Inicio de la UI de Configuración o de las CSA de videovigilancia.
4. Las tareas recién creadas estarán accesibles a través de la barra de tareas de la UI de Configuración o de la UI de Monitoreo.
5. Las tareas similares deberán agruparse en las siguientes categorías:
    a. Funcionamiento: Administración de control de acceso, administración de LRP y otros.
    b. Investigación: Informes de marcadores de video/movimientos/archivo, informes de actividades de control de acceso, informes de actividades de visitantes, informes de alarmas, informes de actividades ALPR, y otros.
    c. Mantenimiento: Informes de configuración de video y control de acceso, solución de problemas, registros de auditoría, informes relacionados con el estado del sistema, y otros.
6. Un operador solo será capaz de ejecutar una tarea específica si cuenta con los privilegios correspondientes.

7. El contenido de la Página de Inicio será personalizable a través del uso de privilegios para esconder tareas a las cuales no debería tener acceso un operador y a través de una lista de tareas favoritas y usadas recientemente. Además, será posible editar un archivo USP XML para agregar nuevas tareas sobre la marcha.

N. El contratista deberá proporcionar hasta XX número de clientes simultáneos. *(Especificador: las conexiones de cliente son simultáneas; se incluyen las primeras 5 conexiones de cliente; especifique la Licencia del Sitio después de 40 conexiones del cliente (solo Enterprise)*

2.15 Configuración de la interfaz de usuario (UI)

A. General:

1. La aplicación de la UI de Configuración deberá permitir al administrador o a los usuarios con los privilegios adecuados cambiar la configuración del sistema. La UI de Configuración deberá proporcionar una configuración y administración descentralizada del sistema de la USP desde cualquier parte de la red IP.

2. La configuración de todos los sistemas ACS, VMS y ALPR embebidos será accesible a través de la UI de Configuración.

3. La UI de Configuración deberá tener una página de inicio con acceso a varias tareas con un solo clic.

4. La UI de Configuración deberá incluir una variedad de herramientas como herramientas para la solución de problemas, herramientas de importación, y una herramienta de detección de unidad, entre otras.

5. La UI de Configuración deberá incluir una interfaz de generación de informes estática para:

   a. Ver eventos históricos basado en la actividad de la entidad. El usuario será capaz de desempeñar acciones como imprimir un informe y solucionar un problema de un evento de acceso específico desde la vista de la generación de informes.

   b. Visualizar registros de auditoría que muestran un historial de los cambios que un usuario/administrador han hecho a una entidad.

6. Todos los sistemas embebidos (ACS, VMS y ALPR) podrán volver a usar las entidades comunes como usuarios, cronogramas, alarmas y muchos más.

B. Sistema de administración de videos:

1. La UI de Configuración deberá permitir al administrador o a los usuarios con los privilegios adecuados cambiar la configuración de video.

2. La UI de Configuración deberá proporcionar la habilidad de cambiar la calidad, ancho de banda y parámetros de velocidad de cuadro del video cámara por cámara (flujo) tanto para video en vivo como grabado.

3. La UI de Configuración deberá proporcionar la habilidad de cambiar la calidad del video con una selección de plantilla de calidad de video predefinida.

4. La UI de Configuración deberá proporcionar la habilidad de configurar los parámetros de brillo, contraste y matiz para cada cámara en el mismo DVS.
5. La UI de Configuración deberá proporcionar la capacidad de habilitar la grabación de audio en las unidades DVS que soportan audio.
6. La UI de Configuración deberá proporcionar la habilidad de cambiar los parámetros de audio, el puerto de serie y la configuración E/S de unidades DVS individuales.
7. La UI de Configuración deberá proporcionar la capacidad de renombrar todas las unidades DVS con base a la topología del sistema y para agregar información descriptiva para cada DVS.
8. La UI de Configuración deberá proporcionar la habilidad de establecer cronogramas y modos de grabación para cada cámara individual. El modo de grabación puede ser:
    a. Continuo
    b. En movimiento o Manual
    c. Solo manual
    d. Desactivado
9. La UI de Configuración deberá soportar la creación de cronogramas para los cuales se puede adjuntar los siguientes aspectos funcionales:
    a. Calidad de video (para cada transmisión de video por cámara)
    b. Grabación (para cada cámara)
    c. Detección de movimientos (para cada zona de detección por cámara)
    d. Brillo, Contraste y Matiz (para cada cámara)
    e. Ejecución de secuencia de cámara
10. La UI de Configuración deberá soportar la creación de cronogramas de grabación ilimitados y asignar cualquier cámara a cualquier cronograma.
11. La UI de Configuración deberá detectar y advertir al usuario de cualquier conflicto dentro de los cronogramas asignados.
12. La UI de Configuración deberá ofrecer la capacidad de configurar un protocolo PTZ a un puerto en serie DVS específico y permitirá la mezcla de domos de varios fabricantes dentro del sistema.
13. Los usuarios tendrán la habilidad de configurar una función de retornar a la página de inicio después de un período de tiempo predefinido de inactividad para las cámaras PTZ. El período de inactividad deberá ser configurable de 1 a 7200 segundos.

2.16 Interfaz de usuario (UI) de cliente VMS

A. La UI de Monitoreo deberá satisfacer la función de una Interfaz Unificada de Seguridad capaz de monitorear eventos de video, ALPR y control de acceso, al igual que visualizar video en vivo y grabado.

B. La UI de Monitoreo deberá proporcionar una interfaz de usuario gráfica para controlar y monitorear la USP sobre cualquier red IP. Deberá permitir a los administradores y operadores con los privilegios adecuados monitorear su plataforma unificada de seguridad, ejecutar informes y administrar alarmas.

C. Para mejorar la usabilidad y la eficiencia del operador, la UI de Monitoreo deberá soportar los siguientes conceptos de UI:

1. Interfaz adaptable de forma dinámica que se ajusta en tiempo real a lo que está haciendo el operador.

2. Una sección de controles dinámicos equipada con widgets específicos de las entidades (como widgets para puertas y cámaras).

3. Uso de superposiciones transparentes que puedan mostrar múltiples tipos de datos de manera transparente.

4. Visualización de menús de recuadros y comandos rápidos.

5. Flujos de trabajo consolidados y consistentes.

6. Menús de recuadros y comandos rápidos de fácil acceso dentro de cada recuadro visualizado del área de trabajo del usuario.

7. Funcionalidad con un solo clic para generación de informes y rastreo. La UI de Monitoreo deberá soportar tanto la generación de informes para el control de acceso, ALPR y videos con un solo clic, así como el rastreo de áreas, cámaras, puertas, zonas, tarjetahabientes, elevadores, entidades ALPR, y otras con un solo clic. La generación de informes y rastreo con un solo clic deberá crear una nueva tarea con las entidades seleccionadas a reportar o rastrear.

D. Página de Inicio y Tareas de la UI de Monitoreo:

1. Las tareas similares deberán agruparse en las siguientes categorías:

a. Funcionamiento: Control de acceso/LRP/videovigilancia, administración de visitantes, aglomeraciones, monitoreo de control de acceso y alarmas de videos, y otros.

b. Investigación: Informes de marcadores de video/movimientos/archivo, informes de actividades de control de acceso, informes de actividades de visitantes, informes de alarmas, informes de actividades ALPR, y otros.

c. Mantenimiento: Informes de control de acceso y configuración de videos, solución de problemas, registros de auditoría y mucho más.

E. UI Adaptable de Forma Dinámica, sección de Controles y Widgets:

1. La UI de Monitoreo deberá adaptarse de forma dinámica a lo que está haciendo el operador. Esto se puede lograr a través de la agrupación de widgets en la sección de Controles de la UI de Monitoreo.
2. Los widgets deberán ser miniaplicaciones o miniagrupaciones en la sección de Controles de la UI de Monitoreo que permitan al operador desempeñar tareas comunes y proporcionarles un rápido acceso a información y acciones.
3. Con un solo clic sobre una entidad (como una puerta o cámara), aparece el widget específico asociado a dicha entidad y el resto de los widgets no relevantes desaparecen de forma dinámica (al instante). Los widgets le ofrecerán al operador información como el estado de la puerta e información de los flujos de las cámaras, al igual que acciones del usuario, como desbloqueo de puertas, controles PTZ, y otros.
4. Los widgets específicos incluyen aquellos para una puerta, cámara, alarma, zona, recuadro de visualización, transmisión de video (estadísticas), cámara PTZ, y otros.

F. Flujos de Trabajo del Operador:

1. Un flujo de trabajo será una secuencia de operaciones que deberá ejecutar un operador o administrador para completar una actividad. El “flujo” se relaciona a una escala de tiempo o secuencia definida claramente para ejecutar la actividad.
2. La UI de Monitoreo deberá estar equipada con flujos de trabajo consistentes para ALPR, videos, y sistemas de control de acceso a los cuales unifica.
3. Generar o imprimir un informe, configurar o reconocer una alarma, o crear un informe de incidente deberá seguir el mismo proceso (flujo de trabajo) sin importar si el operador está trabajando con video, ALPR o control de acceso, o bien con ambos, video y control de acceso.

G. Cada tarea dentro de la UI de Monitoreo deberá consistir de uno o más de los siguientes elementos:

1. Lista de eventos.
2. Árbol lógico: Las puertas, las cámaras, las zonas, las unidades ALPR y los elevadores deberán estar agrupados bajo Áreas de una forma jerárquica.
3. Lista de entidades de todas las entidades que están siendo rastreadas.
4. Visualizar recuadros con varios patrones (1 x 1, 2 x 2, y otros).
5. Visualizar los menús de recuadros con varios comandos relacionados con cámaras, puertas, PTZ y controles de recuadros.
6. Sección de controles con widgets.

H. La UI de Monitoreo deberá soportar múltiples listas de eventos y patrones de recuadros de visualización, entre los que se incluyen:

1. Solo el diagrama de las listas de eventos/alarmas
2. Solo el diagrama de los recuadros de visualización

3. Combinación de las listas de alarmas/eventos y recuadros de visualización
4. Combinación de las listas de alarmas/eventos y mapas ALPR

I. Personalización del área de trabajo del usuario

1. El usuario tendrá el control completo sobre el área de trabajo del usuario a través de una variedad de opciones de personalización seleccionadas por el usuario. Los administradores también serán capaces de limitar lo que los usuarios y operadores pueden modificar en su área de trabajo a través de privilegios.
2. Una vez personalizado, el usuario será capaz de guardar su área de trabajo.
3. El área de trabajo del usuario será accesible por un usuario específico desde cualquier aplicación de cliente en la red.
4. Los patrones de recuadros de visualización se podrán personalizar.
5. Las listas de eventos y alarmas se podrán colocar en cualquier parte de la pantalla, desde sólo una parte de la pantalla hasta la pantalla completa, y el usuario podrá cambiar su tamaño. La longitud de las listas de eventos o alarmas deberán ser definidas por el usuario. Las barras de desplazamiento deberán permitir al usuario navegar a través de largas listas de eventos y alarmas.
6. La UI de Monitoreo deberá soportar varios patrones de mosaicos de visualización, por ejemplo, un mosaico de visualización (matriz 1x1), 16 mosaicos (matriz 8x8) y otras variaciones.
7. La UI de Monitoreo deberá soportar tantos monitores como adaptadores de video de PC y el Sistemas Operativo Windows que sea capaz de aceptar.
8. Las opciones de personalización adicionales incluyen mostrar/ocultar paneles de ventana, mostrar/ocultar menús/barras de herramientas, mostrar/ocultar información superpuesta en videos, cambiar el tamaño de diferentes paneles de ventana y elegir el patrón de visualización de mosaicos por tarea.

J. La UI de Monitoreo deberá proporcionar una interfaz para soportar las siguientes tareas y actividades comunes al control de acceso, ALPR y videos:

1. Monitorear eventos desde un sistema de seguridad en vivo (ACS y/o VMS y/o ALPR).
2. Generar informes, incluyendo informes personalizados.
3. Monitorear y reconocer alarmas.
4. Crear y editar incidentes y generar informes de incidentes.
5. Visualizar mapas gráficos dinámicos y planes de piso al igual que ejecutar acciones desde mapas y planes de piso gráficos y dinámicos.
6. Administrar y ejecutar acciones y macros actuales.

K. La UI de Monitoreo será capaz de monitorear la actividad de las siguientes entidades en tiempo real: áreas, entidades ALPR, puertas, elevadores, cámaras, tarjetahabientes, grupos de tarjetahabientes, zonas (puntos de entrada), y otros.

L. La UI de Monitoreo deberá incluir capacidades avanzadas de videos, entre las que se incluyen:

1. Funcionalidad de visualización avanzada de videos en vivo.
2. Funcionalidad de reproducción avanzada de archivos y reproducción de videos.
3. Monitoreo y administración de eventos y alarmas del sistema de videos.
4. Intercomunicador o audio dúplex
5. Generación de informes de video.
6. Control de cámaras PTZ.
7. Creación y monitoreo de solicitudes de transferencia de archivos.
8. Visualización de superpuestos de metadatos en video en vivo o en modo de reproducción.

M. La UI de Monitoreo deberá aprovechar la Unidad de Procesamiento Gráfico (GPU, por sus siglas en inglés) para la decodificación de video.

1. Se deberán soportar las siguientes tecnologías GPU:
   a. NVidia CUDA
   b. Intel Quick Sync
2. La UI de Monitoreo deberá contar con la habilidad de decodificar video a través del uso simultaneo del GPU y las Unidades de Procesamiento de la Computadora (CPU).

N. Las capacidades de visualización de video en vivo de la UI de Monitoreo deberán incluir:

1. La habilidad de visualizar todas las cámaras vinculadas a la USP y todas las cámaras vinculadas a los sistemas federados.
2. Soporte para el monitoreo de video en vivo en todos y cada uno de los recuadros de visualización dentro de una tarea en el área de trabajo del usuario.
3. La USP deberá soportar la transmisión de video sin interrupción. La CSA deberá mantener las conexiones de video existentes activas en caso de que un SSM (con excepción del Archiver) no esté disponible.
4. La habilidad para arrastrar y soltar una cámara en un recuadro de visualización para la visualización en vivo.
5. La habilidad para arrastrar y soltar una cámara dentro de un recuadro de visualización para la visualización en vivo en un monitor analógico conectado a un decodificador de hardware IP (convierte un flujo encriptado IP en una señal de video analógica).
6. La habilidad para arrastrar y soltar una cámara de un mapa a un recuadro de visualización para la visualización en vivo.

7. Soporte para el zoom digital de las transmisiones de video en vivo de las cámaras.
8. La habilidad para comunicación de audio con unidades de video con entrada y salida de audio.
9. La habilidad para controlar el zoom de panorámica e inclinación, iris, enfoque y preestablecidos.
10. La habilidad para marcar eventos importantes para la recuperación posterior de cualquier cámara de archivado y para nombrar de forma única cada marcador con el fin de facilitar búsquedas futuras.
11. La habilidad para iniciar/detener la grabación en cualquier cámara en el sistema que está configurada para permitir la grabación manual al hacer clic en un solo botón.
12. La habilidad para activar o desactivar la visualización de todos los eventos del sistema a medida que ocurren.
13. La habilidad de cambiarse a reproducción inmediata de video para cualquier cámara de archivado con el simple clic de un botón.
14. La habilitad de tomar instantáneas de videos en vivo y ser capaz de guardar o imprimir dichas instantáneas.
15. La habilidad para ver la misma cámara varias veces en diferentes recuadros.

O. Las capacidades de reproducción de video (reproducción de archivo) de la UI de Monitoreo deberán incluir:

1. Soporte para la reproducción de audio y video para cualquier intervalo de tiempo.
2. Soporte para la reproducción de video de todos y cada uno de los recuadros de visualización.
3. La habilidad de reproducir de forma instantánea el video para cualquier cámara de archivado con el simple clic de un botón.
4. La habilidad para seleccionar entre la sincronización instantánea de todas las transmisiones de video en el modo de reproducción, lo que permite que los operadores visualicen eventos desde múltiples ángulos o a lo largo de varios campos de cámara, o en reproducción asíncrona.
5. La habilidad para visualizar de manera simultánea la misma cámara en múltiples recuadros en diferentes intervalos de tiempo.
6. La habilidad de controlar la reproducción con:
    a. Pausa
    b. Bloqueo de Velocidad
    c. Reproducción Hacia Adelante y Hacia Atrás: 1x, 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x

d. Reproducción Hacia Adelante y Hacia Atrás cuadro por cuadro

e. Reproducción Lenta Hacia Adelante y Hacia Atrás: 1/8x, 1/4x, 1/3x, 1/2x

f. Reproducción de bucle entre dos marcadores de tiempo

7. La habilidad de visualizar una sola escala de tiempo o una escala de tiempo para cada transmisión de video seleccionado, la cual permitirá al operador navegar a través de la secuencia de video simplemente haciendo clic sobre cualquier punto en la escala de tiempo.
8. La habilidad de visualizar el nivel de movimiento en cualquier punto de la escala de tiempo.
9. La habilidad de visualizar de forma clara los eventos marcados en la escala de tiempo.
10. La habilidad de consultar videos archivados usando varios criterios de búsqueda que incluyen, pero que no se limitan a, hora, fecha, cámara y área.
11. La herramienta necesaria para la búsqueda de video y audio asociado con base a eventos definidos por el usuario o a parámetros de movimiento.
12. La habilidad para definir un área del campo del video en la cual buscar el movimiento, así como definir la cantidad de movimiento que activará los resultados de la búsqueda. La UI de Monitoreo deberá entonces recuperar todas las transmisiones de video archivadas que contienen el movimiento que cumple con los parámetros buscados. Deberá existir una escala de tiempo gráfica sobre la cual se deberá indicar el acierto de cada búsqueda.
13. La habilidad para navegar a lo largo de una lista de todos los favoritos creados en el sistema y seleccionar cualquier evento favorito para su visualización.
14. La habilidad de agregar favoritos a video archivado anteriormente para una búsqueda y recuperación más fácil.
15. Soporte para el zoom digital en reproducción de transmisiones de video.
16. Exportación de imágenes fijas a formato PNG, JPEG, GIF, y BMP con el sello de Fecha y Hora, y Nombre de la Cámara en la imagen (instantánea).
17. Herramientas para la exportación de video y reproductor de video auto contenido en varios medios como claves USB o CD/DVD-ROM. Este reproductor de video deberá ser fácil de usar sin entrenamiento y deberá seguir soportando la revisión de meta datos de video, como por ejemplo, los favoritos, o navegar por el video con funciones como la corrección de distorsión de la visualización panorámica de la cámara.
18. Herramientas para la exportación de secuencias de video en formatos estándar de video, tales como ASF o MP4.
19. La habilidad para encriptar archivos de video exportados.
20. La habilidad para que un operador cargue archivos de video previamente exportados desde su computadora o red.

21. La habilidad para guardar consultas al cerrar la CSA y volver a aparecer cuando se vuelve a abrir la aplicación.
22. La habilidad para bloquear de forma dinámica, a petición, transmisiones de video a usuarios de menor nivel para evitar el acceso, por un período de tiempo específico, a video en vivo y grabado.
23. Una herramienta de construcción y exportación de un juego de videos a un solo contenedor. Esta herramienta deberá permitir al operador reunir secuencias de video para crear un guion gráfico y permitir la exportación de cámaras sincrónicas.
24. La habilidad de almacenar el video exportado y la imagen fija exportada a una ubicación de almacenamiento previamente definida.
25. Una interfaz con la habilidad de listar, buscar y manipular exportaciones de video generadas con anterioridad.
26. La habilidad de exportar secuencias de video en estándares abiertos incluyendo ASF y MP4.

P. La UI de Monitoreo deberá ofrecer una interfaz para soportar las siguientes tareas y capacidades de ALPR:

1. Monitoreo y administración de eventos ALPR y alarmas.
2. Visualización de foto(s) de placas de matrícula e imágenes de contexto.
3. Visualización de información de placas de matrícula (por ejemplo, lecturas de las placas de matrícula)
4. Verificación de datos ALPR contra video en vivo y grabado.

Q. Monitoreo de la Entidades:

1. La USP deberá permitir al usuario seleccionar múltiples entidades a monitorear desde la UI de Monitoreo al agregar las entidades una por una a la lista de seguimiento.
2. La UI de Monitoreo deberá ofrecer la opción de filtrar cuáles eventos deberán visualizarse en el diagrama de los recuadros de visualización y/o el diagrama de la lista de eventos.
3. Deberá ser posible bloquear un recuadro de visualización de la UI de Monitoreo de manera que solo rastree la actividad de una entidad específica (como una puerta o cámara específica).
4. El usuario deberá ser capaz de arrastrar y soltar un evento desde una lista de eventos (o una alarma de una lista de alarmas) en un recuadro de visualización para ver una lectura de placa de matrícula , la foto que identifica al tarjetahabiente, la tarjeta de identificación, o video en vivo/archivado, entre otras opciones.
5. Las listas de eventos, alarma, monitoreo/rastreo y listas de informes deberán contener las fotos del tarjetahabiente cuando corresponda.

6. El usuario tendrá permitido iniciar o poner en pausa la visualización de eventos dentro de cada recuadro de visualización.

R. Visualización de Empaquetado y Desempaquetado de Mosaicos:

1. La UI de Monitoreo deberá soportar el empaquetado y desempaquetado con un solo clic para los aciertos ALPR, lecturas ALPR, áreas, puertas, zonas, secuencias de cámaras y alarmas.

2. El empaquetado y desempaquetado de entidades permitirá a los operadores obtener rápidamente información adicional y vistas de cámara de una entidad específica.

3. El desempaquetado de una entidad deberá mostrar las entidades relacionadas. Por ejemplo, el desempaquetado de una puerta con múltiples cámaras asociadas deberá mostrar todas las cámaras asociadas con dicha puerta. El desempaquetado deberá volver a configurar los recuadros de visualización para que puedan mostrar todas las entidades asociadas. Por ejemplo, el desempaquetado de una puerta (o una zona o alarma) que tiene actualmente una configuración de recuadro 1 x 1 y que tiene 3 cámaras enlazadas a la misma creará un diagrama de recuadro de visualización de 1 x 3 para la visualización de todas las entidades asociadas.

4. El empaquetado devolverá la visualización al patrón original del recuadro.

S. Rastreo de Informes:

1. La UI de Monitoreo deberá soportar la habilidad de rastrear de forma manual un objetivo móvil con el solo clic de un botón.

2. La habilidad de cambiar la vista de una cámara a una cámara adyacente deberá hacerse dentro de un solo recuadro de visualización.

3. El intercambio de flujos de cámara deberá lograrse al hacer simplemente un clic sobre una forma semi-transparente o una superposición.

4. Deberá estar disponible el rastreo visual con video en vivo y grabado.

2.17 Requisitos de la Interfaz de Usuario del Administrador del Servidor

A. El Administrador del Servidor se usará para configurar el SSM y la Función de Directory (configuración principal) y su(s) base(s) de datos para aplicar la licencia, y otros más.

B. El Administrador del Servidor será una aplicación basada en la Web. A través del Administrador del Servidor será posible tener acceso al SSM a lo largo de la red o de forma local en el servidor.

C. El acceso al Administrador del Servidor estará protegido a través de un nombre de inicio de sesión, contraseña y comunicaciones encriptadas.

D. El Administrador del Servidor deberá permitir al administrador (usuario) realizar las siguientes funciones:

1. Administrar la licencia del sistema.

2. Configurar la(s) base(s) de datos y el servidor de la base de datos para la Función de Directory.
3. Activar/ Desactivar la Función de Directory
4. Respaldar manualmente la(s) base(s) de datos de la Función de Directory y/o restaurar la(s) base(s) de datos del servidor, al igual que configurar las copias de seguridad programadas de las bases de datos.
5. Definir las configuraciones de seguridad de las comunicaciones entre el cliente y el servidor.
6. Configurar el hardware de comunicaciones de la red, incluidos las direcciones y los puertos de conexión.
7. Configurar las configuraciones SMTP del sistema (servidor de correo y puerto).
8. Configurar opciones de almacenamiento de historial de eventos y alarmas.

2.18 Requisitos Generales del Unified Web Client (UWC)

A. La USP deberá soportar un cliente web unificado (UWC, por sus siglas en inglés) para el control de acceso y video.

B. La UWC deberá ser un cliente verdaderamente ligero que no requiera de ninguna descarga con excepción de un navegador de web o plugins estándar de navegador de web.

C. La UWC deberá ser independiente de plataformas y ejecutarse dentro de Microsoft Edge, Internet Explorer, Firefox, Safari y Google Chrome.

D. Las páginas web para el Web Client serán administradas e insertadas por la Función del servidor Web. No será necesario Microsoft IIS ni ningún otro servicio de hospedaje de sitios web debido a que todas las páginas web serán hospedadas por la función del servidor Web.

E. El UWC deberá soportar la visualización en formato de tableta.

F. El UWC deberá soportar videos nativos H.264 en el cliente web.

G. Las páginas web para el Web Client serán administradas e insertadas por el Web Client Server. No será necesario Microsoft IIS ni ningún otro servicio de hospedaje de sitios web debido a que todas las páginas web serán hospedadas por el Mobile Server.

H. El contratista deberá proporcionar hasta XX número de Web Clients simultáneos. *(Especificador: las conexiones de Web Client son simultáneas; se incluyen las primeras 5 conexiones de Web Client; especifique la Licencia del Sitio desp°ués de 40 conexiones de Web Client (solo Enterprise))*

I. El Web Client Server deberá proporcionar la capacidad de definir una URL única para acceder al Web Client, a fin de garantizar la seguridad de la aplicación.

J. El UWC proporcionará la capacidad de cargar un plano de cámara.

K. El UWC proporcionará la habilidad de configurar, guardar y volver a cargar los diagramas privados de la cámara.

L. El UWC proporcionará la habilidad de controlar las Cámaras PTZ.

M. Funcionalidades:

1. El soporte para iniciar sesión estará disponible mediante:
    a. nombre de usuario y contraseña
    b. Active Directory.
    (Especificador, Profesional y superior, se requiere licencia adicional para Active Directory)
    c. Proveedor de identidad Azure Active Directory, ADFS, OpenID Connect o SAML2. *(Especificador, Profesional y superior, se requiere licencia adicional para OIDC y SAML2)*
    d. Posibilidad de que el usuario cambie su contraseña.
2. Comunicaciones encriptadas para todas las transacciones.
3. Impresión de informes y exportación a un archivo CSV.
4. La personalización del logotipo del cliente deberá estar disponible para aplicaciones de múltiples inquilinos y aplicaciones de servicios de hospedaje.
5. Vídeo:
    a. Video en vivo y grabado a 320 x 240, 640 x 480 o 1280 x 1024 a 15 fps
    b. Exportación de vídeo
    c. 1, 4, 6 o 9 mosaicos
    d. Controles PTZ Básicos (Panorámica/Inclinación, Zoom, ver valores preestablecidos e iniciar patrón)
    e. Iniciar/Detener grabación
    f. Página web de muestra para que los clientes vean cómo ver video para su propio desarrollo.
    g. Agregar marcadores
6. Alarmas:
    a. Informe de alarmas
7. Nivel de Amenaza.

2.19 Requisitos Generales para Aplicaciones para Teléfonos Inteligentes y Tabletas

A. La USP deberá soportar aplicaciones móviles para diferentes dispositivos disponibles en el mercado. Las aplicaciones móviles deberán comunicarse con el Mobile Server de la USP a través de cualquier conexión wifi o red celular.

B. Las aplicaciones móviles deberán comunicarse con la USP a través de una función del Mobile Server (MSR, por sus siglas en inglés). Toda comunicación entre las aplicaciones móviles y la MSR estará basada en el protocolo TCP/IP estándar y deberá usar la encriptación TLS con certificados digitales para proteger el canal de comunicación.

C. Los fabricantes de los dispositivos soportados incluyen (consultar las especificaciones de aplicaciones móviles para ver la lista de compatibilidad más reciente):

   1. Dispositivos Apple con iOS 11.0 o más reciente
   2. Dispositivos con Android 6.0 o más reciente

D. Deberá ser posible descargar las aplicaciones móviles desde la tienda de aplicaciones Central (Apple iTunes App Store, Google Play).

E. Deberá ser posible enviar la configuración a los dispositivos móviles a través de una solución de administración de dispositivos móviles como VMWare Workspace One o Microsoft Intune.

F. Funcionalidades:

   1. Principales
      a. Posibilidad de iniciar sesión / cerrar sesión en la USP utilizando un perfil de usuario autorizado del sistema.
      b. Capacidad para admitir la autenticación pasiva de un proveedor de inicio de sesión única (proveedor de identidad OpenID Connect o SAML2).
      c. Posibilidad de utilizar funciones biométricas (huella digital, identificación facial, etc.) para realizar la conexión al sistema.
      d. Posibilidad de modificar la imagen o contraseña del usuario de la Mobile app.
      e. Posibilidad de ver el Nivel de Amenaza actual del sistema.
      f. Posibilidad de modificar el Nivel de Amenaza actual del sistema.
      g. Posibilidad de ejecutar acciones activas configuradas en el perfil del usuario.
      h. Posibilidad de ver entidades de la USP:
         i. Cámeras
         ii. Puertas
         iii. Cámaras ALPR
         iv. Plugins de Mosaicos Web
         v. Planos
         vi. Secuencias de Cámaras
         vii. Macros

viii. Mapas (solo mapas geográficos) *(Especificador, se requiere licencia adicional, Plan Manager Advanced)*

i. Posibilidad de navegar por la vista jerárquica de las entidades del sistema y buscar entidades en el sistema.

2. Vídeo

a. Posibilidad de ver video en vivo y grabado en las cámaras de la USP. Se podrán ver cuatro cámaras como máximo.

b. Posibilidad de ver videos en formato nativo (H.264).

c. Posibilidad de ver en paralelo video en vivo y grabado para una cámara específica.

d. Posibilidad de utilizar zoom digital en las cámaras.

e. Posibilidad de realizar acciones en las cámaras, como agregar un marcador, controlar un PTZ, controlar la función de iris/enfoque, guardar una instantánea e iniciar/detener una grabación.

f. Posibilidad de ver planos de cámaras.

g. Posibilidad de ver secuencias de cámaras.

h. Posibilidad de ejecutar un informe de eventos de cámaras.

i. Posibilidad de modificar la calidad de video de las cámaras que se muestran en la aplicación móvil.

j. Posibilidad de usar la cámara del teléfono inteligente y transmitir una secuencia de video en vivo a una grabadora de video del sistema.

3. Control de Acceso

a. Posibilidad de ver el estado de la puerta y de la cerradura de la puerta.

b. Posibilidad de realizar acciones en una puerta, como desbloquearla, cambiar el modo a modo de mantenimiento y anular el horario de desbloqueo.

4. Reconocimiento Automático de Placas de Matrícula

a. Posibilidad de ver eventos en vivo de una cámara ALPR.

b. Posibilidad de ver la imagen de lectura, la imagen contextual y todos los metadatos que captura la cámara ALPR.

c. Posibilidad de ejecutar un informe de eventos ALPR.

d. Posibilidad de agregar una placa de matrícula a una lista activa del sistema.

5. Administración de alarmas

a. Posibilidad de recibir notificaciones push para notificar a los operadores móviles de la recepción de una alarma.

b. Posibilidad de ver todas las alarmas activas asignadas al operador móvil.

c. Posibilidad de realizar acciones en una alarma, como reconocer, reenviar o alternar el reconocimiento de una alarma activa.

d. Posibilidad de ver entidades vinculadas a la alarma.

6. Mapas *(Especificador, se requiere licencia adicional, Plan Manager Advanced)*

a. Posibilidad de ver mapas geográficos con entidades de la USP localizadas geográficamente en el mapa.

b. Posibilidad de ver cualquier entidad configurada en el mapa.

c. Posibilidad de buscar entidades o ubicaciones en el mapa.

G. Posibilidad de enviar un mensaje desde la interfaz del usuario de clientes a un operador móvil.

H. Posibilidad de enviar una secuencia de video en vivo o grabada desde la interfaz del cliente a un operador móvil.

I. Posibilidad de ver los operadores móviles que hayan habilitado el rastreo de ubicación en un mapa del sistema. La ubicación del operador móvil debería actualizarse en tiempo real. *(Especificador, Plan Manager Advanced, se requiere licencia adicional)*

2.20 Monitor de salud

A. La USP deberá monitorear el estado de salud del sistema, los eventos relacionados con los registros del estado de salud y calcular estadísticas.

B. Los servicios de la USP, funciones, agentes, unidades y aplicaciones de clientes activarán los eventos de los estados de salud.

C. La USP deberá llenar el Registro de Eventos Windows con eventos del estado de salud relacionados con las funciones de la USP, servicios y aplicaciones de clientes.

D. Una función exclusiva, la Función de Monitoreo del Estado de Salud, deberá realizar las siguientes acciones:

1. Monitorear el estado de la salud de todo el sistema y los eventos de registros.

2. Calcular estadísticas dentro de un marco de tiempo específico (horas, días, meses).

3. Calcular la disponibilidad para los clientes, servidores y unidades de videos/acceso/ALPR.

E. Una tarea de Monitoreo del Estado de Salud y una tarea de generación de informes del Historial del Estado de Salud deberá estar disponible para la generación de informes en vivo y de historiales.

F. En la interfaz de usuario de la aplicación cliente, una tarea del tablero de control correspondiente al Monitoreo del Estado de Salud para proporcionar información en vivo, como gráficos circulares y listas de eventos, con el objetivo de evaluar de forma rápida y visual la salud general del sistema.

G. Un tablero de control del estado de salud centralizado basado en la web deberá estar disponible para visualizar las unidades y eventos de funciones del estado de salud de la USP de manera remota.

H. Estadísticas detalladas del cuidado del sistema estarán disponibles a través de un tablero de control basado en la web, y proporcionará métricas del estado de salud de las entidades y funciones de la USP, incluyendo tiempo activo y tiempo promedio entre fallas.

I. Todos los eventos de salud generados en el sistema se pueden usar para automatizar la administración de eventos y acciones de la USP.

J. Los eventos del estado de salud serán accesibles a través del SDK (puede usarse para crear capturas de SNMP).

2.21 Administración de Comunicación (CM) de Session Initiation Protocol (SIP) *(Especificador, se requiere licencia adicional para todas las versiones)*

A. Un operador de la USP será capaz de, dentro de la UI de Monitoreo de la USP, iniciar y responder llamadas desde otros dispositivos de voz de operadores y periféricos como intercomunicador, estaciones de llamadas de emergencia, centros de información, softphones o dispositivos telefónicos.

B. La USP deberá soportar la CM entre la Interfaz de Usuario del cliente de la USP y los dispositivos de extremo SIP.

C. Los dispositivos de extremo SIP deberán ser capaces de registrar a la USP usando un protocolo SIP estándar.

D. La USP deberá soportar la CM entre dos dispositivos extremos SIP.

E. La USP deberá permitir la configuración de conexiones de trunk SIP a múltiples Servidores SIP que soportan los Trunks SIP. *(Especificador: se requiere licencia de Trunk de Sipelia™)*

F. La CM deberá soportar la administración de llamadas hacia y desde otros Servidores SIP conectados mediante Trunks SIP. *(Especificador: se requiere licencia de Trunk de Sipelia™)*

G. La USP debe admitir la configuración de zonas de emisión para anuncios de mensajes pregrabados y en vivo. *(Especificador, se requiere licencia de dirección pública SipeliaTM)*

H. La CM es un servicio de la USP y no deberá requerir la adición de software de terceros.

I. La CM deberá soportar los siguientes códecs de video:

1. H.264
2. H.263
3. H.263 + (1998)

J. La CM deberá soportar los siguientes códecs de audio:

1. PCMA (G.711 aLaw).
2. PCMU (G.711 uLaw).
3. G.722
4. G.729
5. iLBC
6. GSM
7. evento telefónico
8. Speex (Banda estrecha)
9. Speex (Banda ancha)
10. Speex (Banda ultraancha)
11. L.16
12. L.16-44-1
13. G.728
14. G.726-16
15. G.726-24
16. G.726-32
17. G.723
18. G.726-40

K. La CM deberá certificar los dispositivos SIP de los siguientes fabricantes:

1. 2N Telekomunikace
2. Algo
3. Eje
4. Baudisch
5. Castel.
6. Cisco
7. Código Azul
8. Elogiar
9. • EMCOM
10. Grandstream Networks
11. Jacques

12. Mobotix
13. Siedle
14. TalkaPhone
15. Corporación TOA
16. Valcom
17. Vingtor- Stentofon
18. Zenitel
19. Intelbras

L. La CM deberá permitir la grabación bidireccional de audio y video de las sesiones de llamadas. La USP deberá ofrecer las siguientes capacidades de grabación: *(Especificador, se requiere licencia de Sipelia™ Advanced)*

1. La limpieza automática de archivos de sesiones de llamada después de un número de días que se pueden programar.
2. Desactivación de la grabación de llamad entre operadores.
3. Desactivación de la grabación de llamad con operadores específicos.
4. Desactivación de la grabación de llamad con dispositivos de voz específicos.
5. Selección de una ruta de almacenamiento para las grabaciones de sesión de llamada.

M. La CM deberá proporcionar la capacidad de alcanzar una ubicación física identificada por su propio número de extensión, independientemente del usuario conectado a la USP.

N. La CM deberá proporcionar flexibilidad al administrador para definir los puertos de red a ser usados para comunicarse entre los servidores de la USP y lo siguiente:

1. Interfaces de Usuario del Cliente de la USP
2. Dispositivos SIP
3. Servidores SIP

O. La CM deberá ofrecer la capacidad de crear Grupos de Llamadas. Un Grupo de Llamadas es un grupo de números de llamada agrupados bajo un solo número de llamada. Deberá ser posible establecer un Grupo de Llamadas para que llame de forma simultánea o secuencial a los miembros del grupo. El tiempo de permanencia durante el modo de secuencia se podrá configurar.

P. La CM deberá permitir el enrutamiento automático de las llamadas mediante la configuración de un conjunto de reglas (Plan de Marcación de Números Telefónicos). Los Planes de Marcación deberán soportar las siguientes capacidades:

1. Emparejar un número de teléfono con una expresión regular.

2. Enviar llamadas con base al emparejamiento de números telefónicos desde donde se hacen las llamadas.
3. Enviar llamadas con base al emparejamiento del número telefónico de destino.
4. Cambiar la extensión del teléfono desde donde se reciben las llamadas.
5. Cambiar las extensiones de teléfono hacia donde se envían las llamadas.
6. Una combinación de cualquiera de las capacidades anteriores en una prioridad configurada y con base en un cronograma.

Q. Los Planes de Marcación serán aplicables a llamadas entre entidades SIP registradas a la USP y también hacia y desde servidores SIP externos.

R. La USP deberá unificar, dentro de una simple interfaz de usuario, el flujo de trabajo entre las entidades de seguridad asociadas de una sesión de llamada, que incluyen el buzón de llamadas, cámaras, puertas, zonas de intrusión y salidas.

S. La USP deberá soportar video y llamadas de audio:

1. Entre las Interfaces de los Usuarios del Cliente de la USP
2. Hacia y desde las Interfaces de los Usuarios del Cliente de la USP y dispositivos SIP
3. Entre dispositivos SIP

T. La USP deberá proporcionar una interfaz de usuario de administración de llamadas fácil y avanzada que permite a los operadores:

1. Conectar audífonos USB estándar y cámaras web a estaciones de trabajo de la Interfaz de Usuario del Cliente de la USP de manera que los usuarios de la USP puedan hacer llamadas de voz y video a través de la Interfaz de Usuario del Cliente de la USP.
2. Visualizar el video asociado con la llamada y cambiar entre múltiples fuentes de videos.
3. Recibir notificaciones de llamadas entrantes directamente mediante una bandeja de notificación.
4. Iniciar, contestar, enviar, poner en espera, o cancelar llamadas desde un buzón de diálogo de llamadas dedicado.
5. Controlar cámaras, puertas, zonas y salidas de dispositivos durante una llamada.
6. Crear una lista de contactos personalizada, de manera que los usuarios puedan llamar a sus contactos de manera rápida. Las listas de contactos deberán incluir otros usuarios de la USP al igual que dispositivos SIP.
7. Marcar un número de teléfono para hacer una llamada.
8. Marcar una secuencia DTMF durante una llamada.

9. Monitorear el estado de disponibilidad de un usuario y configurar su propio estado de disponibilidad.
10. Tener acceso a un historial de registros de llamadas que el operador inició y recibió. Este registro deberá mostrar la hora de la llamada, duración, dirección y la razón por la que terminó. Deberá ser posible volver a marcar a una de las entradas en el registro.

U. La USP deberá permitir al operador administrar hasta 10 llamadas de forma simultánea. La cola de las llamadas deberá mostrar el estado de cada llamada: entrante, en proceso o en espera. Deberá ser posible poner en espera y reanudar una llamada directamente desde la cola de las llamadas.

V. La USP deberá ofrecer una ventana de llamadas. Dentro de la ventana de llamadas deberá ser posible:

1. Intercambiar entre cámaras asociadas con el participante de la llamada.
2. Abrir y cerrar puertas asociadas con el participante de la llamada.
3. Armar y Desarmar zonas asociadas con el participante de la llamada.
4. Accionar salidas asociadas con el participante de la llamada.
5. Poner en espera, reanudar, reenviar y terminar una llamada.
6. Silenciar el audio del micrófono.
7. Esconder la señal de video de la cámara web.

W. La USP deberá contar con una libreta de direcciones integrada. La libreta de direcciones deberá estar disponible en el buzón de diálogo de llamadas, en donde los usuarios podrán ver y manejar su lista de contactos. Desde la libreta de direcciones, los usuarios podrán hacer lo siguiente:

1. Llamar a un contacto haciendo doble clic sobre el nombre del contacto.
2. Ver el estado de disponibilidad de sus contactos (usuarios y Dispositivos SIP).
3. Visualizar de forma rápida la información de contacto, como la foto, nombre y número.
4. Filtrar sus contactos por tipo (Dispositivo SIP o Usuario).
5. Crear una lista de favoritos al agregar y quitar contactos.
6. Buscar y llamar a los números que aparecen en la lista de contactos.

X. La USP deberá ofrecer un teclado gráfico para marcar números telefónicos que permita al operador hacer llamadas y marcar tonos DTMF durante una llamada.

Y. La USP deberá proporcionar la capacidad de enviar anuncios públicos a través de un micrófono o mensajes pregrabados cargados. Los usuarios podrán hacer lo siguiente:

1. Crear zonas de emisión.

2. Asociar cualquier entidad disponible de SIP a una zona de emisión.
3. Cargar mensajes pregrabados.
4. Activar un mensaje en vivo o pregrabado.

Z. La USP deberá proporcionar capacidades de generación de informes de llamadas para permitir la investigación de actividades durante sesiones de llamadas específicas. El informe deberá proporcionar la capacidad de reproducir grabaciones de audio y ver sesiones de llamadas que tienen videos asociados. El informe de Llamadas deberá proporcionar filtros para hacer consultas a los registros de llamadas por:

1. Fecha y hora
2. Duración de la sesión de llamada
3. Usuarios involucrados y estaciones de llamada
4. Eventos y acciones de llamada
5. Acciones tomadas por un usuario en puertas, zonas de intrusión y salidas durante una sesión de llamadas

AA. La USP deberá dar la capacidad de exportar una sesión de llamadas, que incluye audio bidireccional, video asociado y un diario de registro de la sesión de la llamada.

BB. Deberá ser posible colocar los dispositivos de voz como íconos en un mapa que deberá visualizar el estado de la llamada del dispositivo de voz con un código de color. Un clic con el botón derecho sobre el ícono del dispositivo de voz en el mapa deberá permitir al usuario:

1. Responder o rechazar una llamada entrante.
2. Iniciar una llamada al dispositivo.
3. Poner en espera y reanudar una llamada con el dispositivo

CC. Deberá ser posible que un operador seleccione y transmita su estado de disponibilidad, con los estados de Disponible, Ausente y Ocupado. Este estado deberá aparecer con un código de color en el buzón de diálogo de llamadas de otros operadores.

DD. El Contratista deberá proporcionar hasta XX número de conexiones SIP. *(Especificador: las estaciones SIP se licencian por conexión)*

EE. El Contratista deberá proporcionar hasta XX número de trunks SIP. *(Especificador: los trunk SIP se licencian por tronco; lo normal es 1)*

FF. El Contratista deberá proporcionar una licencia de conmutación por error y grabación bidireccional de audio y video para cada dispositivo SIP. *(Especificador: cada dispositivo con conmutación por error requiere una licencia)*

GG. El contratista deberá proporcionar hasta XX número de direcciones públicas SIP. *(Especificador, la dirección pública SIP es por característica, 1 es el valor típico)*

HH. La CM deberá proporcionar la habilidad de transmitir mensajes de direccionamiento público a una colección de dispositivos SIP incluidos en una zona de emisión. La característica de PA (dirección pública) deberá soportar la siguiente capacidad:

1. Definir zonas de emisión y asignar entidades SIP para cada una de ellas
2. Transmitir mensajes en vivo y pregrabados

2.22 Requisitos Generales de la USP

A. La Plataforma Unificada de Seguridad (USP) deberá ser una solución de software clase empresarial de seguridad y protección habilitada para IP.

B. La USP deberá soportar la unificación transparente del Sistema de Control de Acceso IP (ACS), el Sistema de Administración de Videos IP (VMS), y el Sistema de Reconocimiento Automático de Placas de Matrícula IP (ALPR) bajo una sola plataforma. Las aplicaciones de interfaz de usuario (UI) de la USP deberán presentar una interfaz unificada de seguridad para la administración, configuración, monitoreo y generación de informes de los sistemas embebidos ACS, VMS y ALPR, y dispositivos periféricos asociados.

C. Las funcionalidades disponibles con la USP deberán incluir:

1. La configuración de sistemas embebidos, como los sistemas ACS, ALPR y VMS.
2. El monitoreo de eventos en vivo.
3. El monitoreo de video en vivo y reproducción de video archivado.
4. Administración de alarmas.
5. La generación de informes que incluyan la creación de plantillas de informes personalizados e informes de incidentes.
6. La característica de Federation para el monitoreo global, la generación de informes y la administración de alarmas de múltiples sistemas ACS, VMS y/o ALPR remotos e independientes esparcidos a lo largo de múltiples instalaciones y zonas geográficas. *(Especificador, solo Enterprise, se requiere licencia adicional)*
7. La administración global de tarjetahabientes a lo largo de múltiples instalaciones y zonas geográficas, cada una con su propio sistema ACS independiente. *(Especificador, solo Enterprise, se requiere licencia adicional para cada sitio)*
8. Integración de Microsoft Active Directory para la sincronización de las cuentas de usuarios de la USP y cuentas de tarjetahabientes del ACS. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
9. Dispositivo de intrusión e integración de paneles (monitoreo en vivo, generación de informes y armado/desarmado). *(Especificador, Standard, Professional y versiones superiores, se requiere licencia adicional)*
10. Integración de los dispositivos de Intercomunicador SIP para comunicación bidireccional. *(Especificador, todas las versiones, se requiere licencia adicional)*

11. Integración con sistemas y bases de datos de terceros a través de plug-ins (control de acceso, analíticas de video, puntos de venta, y otros.). *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
12. Visualización de mapas gráficos dinámicos.
13. Integración del sistema de administración de activos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

D. La USP deberá ser instalada en uno o más de los siguientes tipos de instalaciones:

1. Acceso unificado, ALPR, plataforma de videos y cualquier combinación de los mismos.
2. Control de acceso independiente, ALPR o plataforma de video.
3. Acceso unificado y plataforma de video que federa con múltiples ACS, VMS y ALPR remotos.
4. Plataforma independiente de video que federa múltiples VMS remotos independientes.
5. Control de acceso independiente que federa múltiples ACS remotos independientes.
6. Control de acceso independiente que federa múltiples ALPR remotos independientes.

E. Concesión de licencias:

1. Se deberá aplicar una sola concesión de licencias central en el servidor de configuración.
2. No deberá existir un requisito de aplicar una licencia en todo servidor de computadora o estación de trabajo de cliente.
3. Con base en las opciones seleccionadas, se podrán habilitar o deshabilitar uno o más sistemas embebidos.

F. Requisitos de Hardware y Software:

1. Los sistemas de la USP y los embebidos (video, reconocimiento de placas de matrícula y control de acceso) deberán estar diseñados para ejecutarse sobre una plataforma estándar basada en PC equipada con el sistema operativo Windows. El sistema operativo preferido deberá ser coordinado con el Propietario siguiendo los sistemas operativos soportados por el fabricante.
2. El software básico del cliente/servidor será desarrollado en su totalidad usando la plataforma de software .NET de Microsoft y el lenguaje de programación C# (C-Sharp).
3. El(los) servidor(es) de base de datos de la USP deberá(n) estar desarrollado(s) sobre el Servidor SQL de Microsoft. La versión SQL preferida deberá coordinarse con el Propietario y ser compatible con la USP.

4. La USP deberá ser compatible con los ambientes virtuales, incluyendo VMware y Microsoft Hyper-V.

5. La USP deberá usar el desarrollo y las tecnologías de programación más recientes de interfaz de usuario (UI) como lo son Microsoft WPF (Windows Presentation Foundation), el lenguaje de marcado XAML, y la plataforma de software .NET.

2.23 Arquitectura de la USP

A. La USP estará basada en un modelo de cliente/servidor. La USP deberá consistir de un Módulo de Software de Servidor (SSM) estándar y Aplicaciones de Software del Cliente (CSA).

B. La USP deberá ser una solución habilitada para IP. Toda la comunicación entre el SSM y la CSA estará basada en el protocolo TCP/IP estándar y deberá usar la encriptación TLS con certificados digitales para proteger el canal de comunicación.

C. El SSM deberá ser un servicio Windows que se pueda configurar para que comience a funcionar cuando se inicia y ejecuta el sistema operativo en el fondo. El SSM deberá comenzar a funcionar automáticamente cuando se enciende la computadora sin importar si hay o no un usuario con sesión iniciada en la máquina.

D. Los usuarios podrán implementar el SSM en un solo servidor o a lo largo de varios servidores para una arquitectura distribuida. La USP no tendrá restricciones en cuanto al número de SSM instalados.

E. La USP deberá soportar el concepto de la característica de Federation en donde se pueden enlazar múltiples instalaciones independientes ACS, VMS y ALPR en un solo sistema virtual grande para el monitoreo, generación de informes y gestión de alarmas centralizados. *(Especificador, solo Enterprise, se requiere licencia adicional)*

F. La USP deberá proteger contra la posible falla del servidor de la base de datos y continuar funcionando con soluciones estándar disponibles en el mercado .

G. La USP deberá soportar hasta mil instancias de CSA conectadas al mismo tiempo. Sin embargo, se puede instalar un número ilimitado de CSA en cualquier momento. *(Especificador, máximo 5 con Standard; máximo 10 con Professional; ilimitado con Enterprise)*

H. La USP deberá soportar un número ilimitado de registros e historial de transacciones (eventos y alarmas) con el máximo permitido limitado por la cantidad de disco duro disponible.

I. La USP deberá soportar la transmisión de video sin interrupción. La CSA deberá mantener las conexiones de video existentes activas en caso de que un SSM (con excepción del Archiver) no esté disponible.

J. Arquitectura con Base en Funciones:

1. La USP deberá consistir de una arquitectura con base en funciones, donde cada SSM hospeda una o más funciones.

2. Cada función deberá ejecutar un conjunto específico de tareas relacionadas al sistema principal, el reconocimiento automático de placas de matrícula automotriz (ALPR), videos (VMS) o funcionalidades de control de acceso (ACS), entre muchas otras más. La instalación deberá estar simplificada a través de la habilidad de la USP para permitir a los administradores:
    a. Instalar uno o varios SSM a lo largo de la red antes de activar las funciones.
    b. Activar y desactivar funciones según sea necesario en todos y cada uno de los SSM.
    c. Centralizar la configuración y administración de la función.
    d. Soporte de configuración remota.
    e. Mover las funciones desde un SSM a otro.
3. Cada función, cuando sea necesario, deberá tener su propia base de datos para almacenar eventos e información de configuración específica a la función.
4. Las funciones sin base de datos, como la característica de Federation, Active Directory, y Administración Global de Tarjetahabientes, deberán soportar el modo de espera muy próximo al tiempo real sin que se requiera software de conmutación por error de terceros.
5. Función del Directory:
    a. La Función de Directory deberá administrar la base de datos central que contiene toda la información del sistema y la configuración de componentes de la USP.
    b. La Función de Directory deberá autenticar usuarios y dar acceso a la USP con base en derechos o privilegios de acceso predefinidos del usuario y configuraciones de particiones de seguridad.
    c. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes comunes a los subsistemas del ACS, ALPR y el VMS:
        i. Particiones de seguridad, usuarios y grupos de usuarios
        ii. Áreas
        iii. Zonas, reglas de enlace de entrada/salida (E/S) y comportamiento de salida personalizado
        iv. Alarmas. Horarios y tareas programadas
        v. Eventos personalizados
        vi. Macros o guiones personalizados
    d. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al VMS:
        i. Servidores de video y sus periféricos (como audio, E/S y puertos serie)
        ii. PTZ.

iii. Secuencias de cámaras

iv. Horarios de grabación y archivamiento

e. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al ACS:

i. Controladores de puertas, y módulos de entrada y salida (E/S)

ii. Puertas, Elevadores y Reglas de acceso

iii. Tarjetahabientes y grupos de tarjetahabientes, credenciales y plantillas para distintivos

f. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al ALPR:

i. Unidades y cámaras ALPR

ii. Listas activas, listas de permisos y reglas de sobretiempo

6. La Función del Video Archiver será responsable de administrar las cámaras y los codificadores que controle y archive.

7. La Función del Media Router será responsable de enrutar los flujos de video y audio en redes locales y de área extensa, desde la fuente (como el DVS) hacia el destino (como la CSA).

8. La Función del Administrador de Acceso será responsable de la sincronización de las unidades de hardware de control de acceso bajo su control, como lo son los controladores de puerta y los módulos de E/S. Además esta función debe ser responsable de validar y registrar todas las actividades y eventos de acceso cuando los controladores de puertas y los módulos E/S están en línea.

9. La Función del Reconocimiento Automático de Placas de Matrícula (ALPR) será responsable de sincronizar las unidades fijas ALPR (cámaras) y aplicaciones ALPR móviles bajo su control. La Función de ALPR será responsable de registrar todas las actividades y eventos del ALPR.

10. La Función de Zone Manager será responsable de administrar todas las zonas de software (recopilación de entradas) y el registro de eventos de zona asociados. Las zonas deberán consistir de entradas de control de acceso y de dispositivos de video.

11. La Función de Monitoreo del Estado de Salud será responsable por el monitoreo y registro de eventos y advertencias del estado de salud desde varias aplicaciones de cliente, funciones, y servicios que forman parte de la USP. Esta función también será responsable de registrar eventos dentro del Windows Event Log y por generar informes sobre las estadísticas y el historial de salud.

12. Funciones Opcionales:

a. La Característica de Federation™ será responsable de crear un gran sistema virtual que consista de cientos o miles de sistemas ACS, VMS y/o ALPR independientes y remotos. *(Especificador, solo Enterprise, se requiere licencia adicional)*

b. La Función del Global Cardholder Synchronizer será responsable de sincronizar la información de los tarjetahabiente y credenciales entre el sitio local y el sitio central. También deberá soportar la sincronización entre sitios remotos. *(Especificador, solo Enterprise, se requiere licencia adicional)*

c. La Función del Active Directory será responsable de sincronizar las cuentas de los usuarios y cuentas de los tarjetahabientes con un servidor Microsoft Active Directory. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

d. La Función del Intrusion Manager será responsable de administrar los dispositivos de intrusión de terceros como los paneles de alarmas y dispositivos de detección de perímetros. Esta función también será responsable de registrar de todos los eventos de intrusión en una base de datos. *(Especificador, Standard, Professional y versiones superiores, se requiere licencia adicional)*

e. La Función del Asset Manager será responsable de integrar y sincronizar los sistemas de administración de activos de terceros y eventos relacionados con el registro de activos. La función será responsable de soportar la ejecución de informes relacionados con activos como informes de inventarios e informes de actividad de activos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

f. El Rol de Plug-in Manager será responsable por la comunicación entre la USP y los sistemas de terceras partes como lo son analítica de video, el control de acceso, los ALPR, los videos y los sistemas de administración del edificio. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

g. La Función del Point of Sale (POS, por sus siglas en inglés) será responsable de integrar la USP con sistemas POS de terceros y de registrar las transacciones. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

h. La Función de Web SDK será responsable de conectar la USP a cualquier aplicación o interfaz desarrollada con el Web Service SDK. Las aplicaciones desarrolladas con el Web Service SDK serán independientes de la plataforma y dependerán del protocolo REST para las comunicaciones. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

i. La Función Communication Management será responsable de registrar los extremos de comunicación SIP y por administrar el enrutamiento de las llamadas. *(Especificador, todos los paquetes, se requiere licencia adicional)*

j. La función del servidor Web actúa como un proxy para las conexiones del cliente y puede ser instalado en un DMZ para obtener seguridad adicional. La función del Web Server actúa como un proxy para las Conexiones de Cliente y puede instalarse en un DMZ para obtener seguridad adicional.

k. La Función de Media Gateway será responsable de conectar cualquier transmisión de video a un sistema de terceros que use el protocolo estándar RTSP/RTSPS. Esta función proporcionará acceso a video en vivo y

reproducción. *(Especificador, Professional y versiones superiores, se requieren paquetes de SDK, se requiere licencia adicional)*

K. Servicio de Monitoreo de Servidores (Watchdog):

1. La USP deberá incluir un Servicio de Monitoreo de Servidores que monitoree continuamente el estado del servicio del Módulo de Software del Servidor (SSM).
2. El Servicio de Monitoreo de Servidores será un servicio Windows que se inicia de forma automática en el encender el sistema, sin importar si el usuario está conectado o no a su cuenta.
3. El Servicio de Monitoreo de Servidores estará instalado en todos los servidores y PC que ejecutan un SSM. En caso de fallas o funcionamiento defectuoso, el Servicio de Monitoreo de Servidores deberá reiniciar el servicio averiado. Como último recurso, el Servicio de Monitoreo de Servidores deberá reiniciar el servidor/PC si no fuera posible reiniciar el servicio.

2.24 Control de acceso USP, video y unificación ALPR

A. El Monitoreo UI deberá presentar una verdadera Interfaz de Seguridad Unificada para el monitoreo y los informes en vivo del ACS, el VMS y el ALPR. La visualización y reproducción avanzada de vídeo en vivo de vídeo archivado deberá estar disponible a través de la UI de Monitoreo.

B. La configuración de UI deberá presentar una verdadera Interfaz de Seguridad Unificada para la configuración y administración del ACS, el VMS y el ALPR.

C. El usuario deberá ser capaz de asociar una o más cámaras de video a los siguientes tipos de entidad: áreas, puertas, elevadores, zonas, alarmas, paneles de intrusión, cámaras ALPR y más.

D. Será posible ver el video asociado con los eventos de control de acceso cuando se visualiza un informe.

E. Será posible ver el video asociado con los eventos de los paneles de intrusión cuando se visualiza un informe.

F. Deberá ser posible ver el video asociado con los eventos del ALPR cuando se visualice un informe.

G. La USP deberá soportar la siguiente funcionalidad de la Administración de Alarmas:

1. Crear y modificar alarmas definidas por el usuario. Deberá soportar un número ilimitado de alarmas definidas por el usuario.
2. Asignar un cronograma de tiempo o período de cobertura a una alarma. Deberá activarse una alarma solamente si es una alarma válida para el período de tiempo actual.
3. Establecer el nivel de prioridad de una alarma y su umbral de reactivación.
4. Definir si se visualiza video en vivo o grabado, imágenes fijas o una mezcla de estos una vez que se activa una alarma.

5. Proporcionar la habilidad de visualizar video en vivo y grabado dentro del mismo recuadro de video utilizando el modo imagen en imagen (PiP).
6. Proporcionar la habilidad de agrupar alarmas por fuente y por tipo.
7. Definir un período de tiempo después del cual se reconoce de forma automática la alarma.
8. Definir los destinatarios de una alarma. Las notificaciones de alarmas deberán distribuirse a uno o más destinatarios. Los destinatarios deberán recibir un nivel de prioridad que jerarquice el orden de recepción de una alarma.
9. Definir el modo de transmisión de la alarma. Las notificaciones de alarmas se enviarán usando un modo de transmisión secuencial o un modo de transmisión de todo a la vez.
10. Definir si se visualiza la fuente de la alarma, una o más entidades o una página HTML.
11. Especificar si es obligatorio la generación de un informe de incidente durante el reconocimiento.

H. Los flujos de trabajo para crear, modificar, agregar instrucciones y procedimientos, y reconocer una alarma deberán ser consistentes para las alarmas de control de acceso, ALPR y videos.

I. Las alarmas deberán ser federadas, permitiendo la gestión global de alarmas a lo largo de múltiples sistemas independientes USP, ACS, VMS y ALPR.

J. La USP deberá además soportar la notificación de alarmas a una dirección de correo electrónico o a cualquier dispositivo que usa el protocolo SMTP.

K. La habilidad para crear instrucciones relacionadas con las alarmas será soportada a través de la visualización de una o más páginas HTML después de un evento de alarma. Las páginas HTML deberán ser definidas por el usuario y se podrán vincular entre sí.

L. Deberá soportarse el empaque y desempaque de la alarma en donde todas las entidades relacionadas con una alarma se puedan visualizar en la UI de Monitoreo con un simple clic de un botón.

M. El usuario tendrá la habilidad de reconocer alarmas, crear un incidente al reconocer una alarma, y colocar una alarma en el modo repetición.

N. El usuario deberá ser capaz de activar alarmas de forma espontánea según lo que vea en el sistema.

O. Una alarma deberá estar configurada de tal forma que permanezca visible hasta que se reconozca la condición de la fuente.

P. El usuario será capaz de investigar la alarma sin tener que reconocerla.

2.25 Niveles de amenaza de la USP *(Especificador: se requiere licencia adicional; solo Enterprise)*

A. La USP deberá soportar los Niveles de Amenaza para cambiar de forma dinámica el comportamiento del sistema para responder a eventos críticos.

B. Los Niveles de Amenaza deberán activarse y desactivarse por el operador de la CSA con el privilegio adecuado.

C. Los Niveles de Amenaza deberán establecerse en un área o en todo el sistema.

D. Los Niveles de Amenaza afectarán el comportamiento del sistema al ejecutar cualquier acción disponible en la USP, como: activar salida, iniciar la grabación, bloquear cámaras, invalidar la calidad de la grabación, armar una zona, colocar una puerta en un modo de mantenimiento, y otros.

E. Deberán estar disponibles las siguientes acciones específicas con los Niveles de Amenaza:

1. Establecer una autorización de seguridad mínima para restringir o permitir el acceso de tarjetahabientes a áreas específicas además de otras restricciones impuestas por las reglas de acceso.

2. Establecer un nivel de usuario mínimo para cerrar automáticamente la sesión del usuario en la USP.

3. Establecer el modo de lector para cambiar la forma de obtener acceso a las puertas (por ejemplo, tarjeta y PIN, o tarjeta o PIN).

F. Se deberá visualizar una notificación visible en toda la CSA del operador cuando se active un Nivel de Amenaza.

2.26 Tarea de la USP remota

A. La USP deberá proporcionar, mediante una Tarea Remota, capacidades para monitorear y controlar de forma remota el contenido de otras estaciones de trabajo que están ejecutando la CSA (UI de Monitoreo) que forman parte del mismo sistema.

B. La USP deberá soportar aplicaciones para paredes de video al conectar y controlar múltiples estaciones de trabajo y monitores de forma simultánea.

C. La Tarea Remota será una interfaz gráfica que muestra la replicación de la estaciones de trabajo remota que están ejecutando la CSA (UI de Monitoreo).

D. La Tarea Remota deberá permitir la conexión a otras estaciones de trabajo que usan un modo de ancho de banda bajo para recibir instantáneas de datos de video visualizado de forma remota.

E. La Tarea Remota deberá permitir la conexión a otras estaciones de trabajo que usan un modo de espía para permanecer invisibles a la estación de trabajo conectada de forma remota. La opción de modo espía deberá estar disponible para los usuarios con permisos para tener acceso a dicha función.

F. La funcionalidad ofrecida por la capacidad de monitoreo y control remoto deberá incluir:

1. Monitoreo remoto y control del monitoreo y las tareas de monitoreo de alarmas.
2. Habilidad para intercambiar cámaras, puertas y zonas de forma remota en los recuadros de visualización.
3. Habilidad para controlar el video en vivo y en reproducción de forma remota.
4. Habilidad para cambiar el patrón del recuadro de forma remota.
5. Habilitad para crear y eliminar tareas de forma remota.
6. Habilidad para iniciar/detener de forma remota los ciclos de las tareas.
7. Habilidad para ir al modo de pantalla completa de forma remota.
8. Habilidad para guardar y volver a cargar el área de trabajo de forma remota.

2.27 Administración Avanzada de Tareas de la USP

A. La USP deberá soportar una infraestructura para administrar las tareas de la UI de Monitoreo que se usan para el monitoreo en vivo, las actividades diarias y la generación de informes.

B. Los administradores deberán ser capaces de asignar tareas y bloquear el área de trabajo del operador. La administración del usuario de su área de trabajo deberá estar limitada por sus privilegios asignados.

C. Los operadores deberán ser capaces de guardar sus tareas, ya sea como tareas Públicas o tareas Privadas, y en una partición específica. Las Tareas Públicas deberán estar disponibles para todos los usuarios. Las Tareas Privadas solo deberán estar disponibles para el propietario de la tarea.

D. Los operadores deberán ser capaces de compartir sus tareas enviándolas a uno o más usuarios en línea. Los destinatarios deberán tener la opción de aceptar la tarea enviada.

E. Los operadores deberán ser capaces de duplicar una tarea.

2.28 Informes de la USP

A. La USP deberá soportar la generación de informes (informes de base de datos) para el control de acceso, ALPR, videos e intrusión.

B. Todos y cada uno de los informes en el sistema deberá ser una tarea de la USP, cada una asociada con su propio privilegio. Un usuario deberá tener acceso a una determinada tarea de informe si cuenta con los privilegios correspondientes.

C. Los flujos de trabajo para crear, modificar, y ejecutar un informe deberán ser consistentes para los informes de control de acceso, ALPR y video.

D. Los informes deberán ser federados, lo que permite la generación de informes globales consolidados a lo largo de múltiples sistemas independientes USP, ACS, VMS y ALPR.

E. Los informes de control de acceso y ALPR deberán soportar las fotos de los tarjetahabientes y fotos de las placas de matrícula, respectivamente.

F. La USP deberá soportar los siguientes tipos de informes:

   1. Informes de alarmas
   2. Informes específicos de video (archivos, marcadores, movimiento y otros)
   3. Informes de configuración (tarjetahabientes, credenciales, unidades, reglas de acceso, lectores/entradas/salidas y más)
   4. Informes de actividades (tarjetahabientes, grupo de tarjetahabientes, visitantes, credenciales, puertas, unidades, áreas, zonas, elevadores y más)
   5. Informes específicos de ALPR (reproducción de ALPR móvil, aciertos, lecturas de placas, lecturas/aciertos por día, lecturas/aciertos por zona de ALPR y demás)
   6. Informes de actividad del estado de salud y estadísticas del estado de salud
   7. Otros tipos de informes, como informes de visitantes, informes de registros de auditoría, informes de incidentes e informes de horario y asistencia

G. Informes Genéricos, Informes Personalizados y Plantillas de Informes:

   1. El usuario deberá tener la opción de generar informes genéricos desde una lista existente, generar informes desde una lista de plantillas definidas por el usuario, o crear un nuevo informe o una plantilla de informe.
   2. El usuario deberé ser capaz de personalizar informes predefinidos y guardarlos como nuevas plantillas de informe. No existirá la necesidad de una herramienta externa de generación de informes para crear informes personalizados y plantillas de informe. Las opciones de personalización incluirán la configuración de filtros, extensión del informe, y período de tiempo de espera. El usuario también deberá ser capaz de establecer cuales columnas serán visibles en un informe. La clasificación de los datos reportados estará disponible haciendo clic en la columna correspondiente y seleccionando un criterio de clasificación (ascendente o descendente).
   3. Todas las plantillas de informes deberán crearse dentro de la UI de Monitoreo.
   4. Estas plantillas se pueden usar para generar informes sobre un cronograma en formato PDF o Excel.
   5. Un número ilimitado de informes y plantillas personalizadas serán soportados.

H. El diagrama de una tarea de generación de informes deberá consistir de paneles con configuraciones (duración de informe, filtros, mandos ‘ir a’ y ‘restablecer’, etc.), los datos actuales del informe en formato de columna, y un panel con recuadros de visualización. El usuario deberá ser capaz de arrastrar y soltar registros individuales en un informe sobre uno o más recuadros de visualización para ver la foto de identificación de un tarjetahabiente, reproducir una secuencia de video, o un evento ALPR.

I. La USP deberá soportar el filtrado completo de datos para la mayoría de los informes con base en el tipo de entidad, tipo de evento, marca de tiempo del evento, campos personalizados, etc.

J. La tarea de informe tendrá la capacidad de mostrar resultados a través de gráficos, como gráficos de líneas, gráficos de barras, gráficos de barras apiladas, gráficos de anillos y gráficos circulares.

K. El usuario deberá ser capaz de hacer clic sobre una entidad dentro de un informe existente para generar informes adicionales desde la UI de Monitoreo.

L. La USP deberá soportar las siguientes acciones en un informe: imprimir el informe, exportar el informe a un archivo PDF/Microsoft Excel/CSV, exportar los gráficos en formato JPG/PNG y enviar de manera automática por correo electrónico un informe en función de un horario y una lista de uno o más destinatarios.

2.29 Tableros de la USP

A. La USP deberá ser capaz de crear tableros.

B. Los operadores deberán poder ver los tableros si cuentan con los privilegios correspondientes. Los usuarios con los privilegios correspondientes también deberán ser capaces de modificar los tableros.

C. Los tableros del sistema deberán ser una tarea de la USP. Un usuario deberá tener acceso a una tarea específica de tablero si cuenta con los privilegios correspondientes.

D. Los tableros se deberán guardar en una carpeta privada o pública.

E. Un tablero deberá estar formado por un área de trabajo con varios widgets que aparezcan en dicha área. Todos los widgets deberán proporcionar la capacidad de especificar su ubicación y tamaño, un título y un color de fondo, y de ofrecer la capacidad de actualizar su contenido con frecuencia.

F. Tipos de widgets para tableros:

1. Imagen: ofrece la capacidad de mostrar una imagen (JPG, PNG, GIF y BMP) en un tablero.

2. Texto: ofrece la capacidad de mostrar texto en un tablero. El estilo del texto deberá poder configurarse, de manera que el usuario pueda especificar la fuente, el tamaño, el color y la alineación.

3. Mosaico: ofrece la capacidad de mostrar cualquier entidad de la USP en un mosaico.

4. Página web: ofrece la capacidad de mostrar una URL en un tablero.

5. Cantidad de entidades: ofrece la capacidad de mostrar la cantidad total de un determinado tipo de entidad en la USP.

6. Informes: ofrece la capacidad de mostrar los resultados de los informes guardados en el sistema. Los resultados se visualizarán mostrando la cantidad

total de resultados en el informe, un conjunto de los principales resultados del informe o un gráfico visual de los datos del informe.

G. Será posible ampliar los widgets de un tablero con un SDK. De esta forma, se podrán desarrollar widgets personalizados para el sistema.

H. La USP deberá soportar las siguientes acciones en un tablero: imprimir el tablero, exportar el tablero a un archivo PNG y enviar automáticamente por correo electrónico un informe en función de un horario y una lista de uno o más destinatarios.

2.30 Característica de Federation de la USP: Monitoreo de sistemas remotos *(Especificador: solo Enterprise, licencia adicional obligatoria para cada sitio y entidad federada.)*

A. La USP deberá soportar el concepto de una función federada para el control de acceso, video y ALPR.

B. La característica de Federation permitirá la unificación de múltiples sistemas USP independientes (sistemas Federados) en un solo sistema virtual más grande (la característica de Federation). Esto deberá facilitar el monitoreo global de múltiples sistemas USP independientes.

C. La característica de Federation deberá soportar la unificación de múltiples sistemas independientes de videovigilancia o VMS.

D. Las entidades que se federarán y monitorearán de forma centralizada desde la característica de Federation deberán incluir alarmas, áreas, cámaras, tarjetahabientes y grupos de configuración de tarjetahabientes, credenciales, puertas, elevadores, eventos ALPR y zonas (entradas monitoreadas).

E. La característica de Federation deberá soportar una integración basada en nube, por medio de la cual se actualizarán de forma automática el servicio e infraestructura y la proporcionará el proveedor del servicio, sin la necesidad de hardware en el sitio.

F. La característica de Federación deberá soportar la Gestión Global de Alarmas, desde el monitoreo de UI para el control de acceso, video y ALPR.

G. La función de federación deberá soportar la Generación Global de Informes desde el monitoreo de UI para el control de acceso, video y ALPR.

H. La característica de Federation deberá soportar docenas de acciones del operador en entidades remotas (federadas) desde la UI de Monitoreo (por ejemplo, generar un informe global tomando en cuenta eventos de múltiples sitios independientes o reconocer alarmas remotas).

2.31 Administración de Zonas de la USP

A. La USP deberá soportar la configuración y administración de las zonas para el monitoreo del punto de entrada a través de la Función del Zone Manager. Un usuario podrá agregar, borrar o modificar una zona si cuenta con los privilegios correspondientes.

B. Una zona deberá monitorear el estado de uno o más puntos de entrada. Deberá ser posible el monitoreo de la zona o de un punto de entrada a través del uso de un controlador y uno o más módulos de entrada. Las entradas desde las cámaras o codificadores de video también deberán estar accesibles a través de una zona.

C. Dependiendo del hardware que está instalado deberán soportarse las entradas supervisadas. Dependiendo del módulo de entrada usado se deberá tener disponibilidad de supervisión tanto de 3 como de 4 estados.

D. Se deberá definir un cronograma para una zona indicando cuándo se monitoreará la zona.

E. Los Eventos Personalizados deberán ofrecer una flexibilidad completa para crear eventos personalizados específicos a una zona. El usuario será capaz de asociar los eventos personalizados a los cambios de estado en las entradas monitoreadas.

F. El ACS deberá soportar una o más cámaras por zona. Videos deberán estar asociados a los cambios de estado de una zona.

G. Enlace de Entrada/Salida (E/S):

1. La administración de las zonas deberá soportar la Vinculación de Entrada/Salida (E/S). El enlace de E/S deberá permitir que una o más entradas activen una o más salidas.

2. El enlace de E/S deberá estar disponible en el modo fuera de línea cuando la comunicación entre el servidor y el hardware no está disponible.

3. Los Comportamientos de Salida Personalizados deberán ofrecer completa flexibilidad para crear una variedad de patrones complejos de señal de salida: pulsos simples, pulsos periódicos, pulsos de ciclo variable, y cambios de estado.

4. A través de la acción de ‘activación de salida’, el ACS deberá soportar la activación de salidas con comportamientos de salida personalizados.

2.32 Administración de Seguridad del Usuario y Grupo de Usuarios, Particiones y Privilegios de la USP

A. La USP deberá soportar la configuración y la administración de usuarios y grupos de usuarios. Un usuario podrá agregar, borrar o modificar un usuario o grupo de usuarios si cuenta con los privilegios correspondientes.

B. La USP deberá soportar la autenticación de usuario con autenticación basada en notificaciones usando proveedores externos. Los proveedores externos deberán incluir:

1. ADFS (Servicios de federación de Active Directory)

2. Azure Active Directory (a través de OpenID Connect)

3. Ping Identity (a través de OpenID Connect)

4. KeyCloak (a través de OpenID Connect)

5. Otros agentes de autenticación de Open ID Connect/SAML2

C. Los derechos y privilegios de acceso comunes compartidos por múltiples usuarios deberán definirse como Grupos de Usuarios. Los miembros individuales del grupo deberán heredar los derechos y privilegios de sus grupos de usuarios primario. Se permitirá el anidamiento de grupo de usuarios.

D. Los privilegios del usuario deberán ser amplios en la USP. Todas las entidades configurables para la USP, incluyendo el control de acceso, video y ALPR, deberán contar con privilegios asociados.

E. Las entidades específicas, como tarjetahabientes, grupos de tarjetahabientes, y credenciales, deberán incluir un juego de privilegios más pormenorizado, como el derecho al acceso a campos personalizados y cambio de activación o estado del perfil de una entidad.

F. Particiones:

1. La USP deberá limitar lo que pueden ver los usuarios en la base de datos de configuración a través de particiones de seguridad (segmentos de base de datos). El administrador, quien cuenta con todos los derechos y privilegios, tendrá permitido segmentar un sistema en múltiples particiones de seguridad.

2. Todas las entidades que forman parte de la USP se pueden asignar a una o más particiones.

3. Un usuario que reciba acceso a una partición específica solo deberá ser capaz de ver las entidades (componentes) dentro de la partición a la cuál ha sido asignado. El acceso se otorga al asignar al usuario como un usuario aceptado para ver las entidades que forman parte de una partición en particular.

4. Un usuario o grupo de usuarios puede recibir derechos de administrador sobre la partición.

G. Deberá ser posible especificar el usuario y los privilegios del grupo de usuarios con base en la partición.

H. Las opciones avanzadas de inicio de sesión deberán estar disponibles como inicio de sesión doble, y otros.

I. Deberá ser posible especificar un período inactivo para la UI de Monitoreo y después de dicho tiempo la aplicación se bloqueará de forma automática, al mismo tiempo que conserva el acceso a las señales de la cámara visualizadas actualmente.

J. Será posible revisar los permisos de los usuarios y determinar lo siguiente:

1. El usuario o grupo de usuarios que pueden ver o modificar una entidad del sistema.

2. Los privilegios de cada usuario o grupo de usuarios del sistema.

3. El usuario o grupo de usuarios que puede realizar la acción vinculada a un privilegio

2.33 Administración de evento/acción de la USP

A. La USP deberá soportar la configuración y la administración de eventos para videos y ALPR. Un usuario será capaz de agregar, eliminar o modificar una acción enlazada a un evento si cuenta con los privilegios correspondientes.

B. La USP deberá recibir todos los eventos entrantes desde uno o más ACS, VMS y/o ALPR. La USP deberá tomar las acciones correspondientes con base a relaciones de eventos/acciones definidas por el usuario.

C. La USP deberá recibir y registrar los siguientes eventos:

1. Eventos en todo el sistema
2. Eventos de aplicación (clientes y servidores)
3. Eventos de áreas, cámaras, puertas, elevadores y ALPR (lecturas y aciertos)
4. Eventos de unidad
5. Eventos de zona
6. Eventos de alarmas
7. Eventos ALPR
8. Eventos de Monitoreo del Estado de Salud

D. La USP deberé permitir la creación de eventos personalizados.

E. La USP deberá contar con la capacidad para ejecutar una acción en respuesta a un evento de control de acceso, video y ALPR. La USP deberá soportar la siguiente lista de acciones, sin estar limitada a:

1. Agregar marcador
2. Activar el área de detección de intrusiones
3. Activar zona
4. Bloquear y desbloquear video
5. Omitir entrada
6. Cancelar la postergación la activación del área de detección de intrusiones
7. Borrar omisión de entrada
8. Borrar tarea
9. Visualizar una cámara en un monitor analógico
10. Visualizar una entidad en la CSA
11. Mandar un informe por correo electrónico
12. Mandar una instantánea por correo electrónico
13. Exportar un informe

14. Obviar la vulneración del antirretorno
15. Ir a la página de inicio
16. Ir a preestablecidos
17. Importar desde archivo
18. Invalidar la calidad de grabación
19. Anular de manera manual con calidad de grabación de evento
20. Anular de manera manual con calidad de grabación manual
21. Reproducir un sonido
22. Postergar la activación de las áreas de detección de intrusiones
23. Reiniciar una unidad
24. Grabación de calidad como configuración estándar
25. Restablecer el conteo de personas en el área
26. Restablecer el inventario de la zona de estacionamiento
27. Ejecutar una macro
28. Ejecutar un patrón
29. Enviar un mensaje
30. Enviar una tarea
31. Enviar un correo electrónico
32. Configure la ocupación de la zona de estacionamientos de
33. Configurar el modo de lector
34. Configurar el modo de mantenimiento de la puerta
35. Establecer un nivel de amenaza
36. Iniciar/detener la aplicación de protección de video
37. Iniciar / detener grabación
38. Iniciar / detener transferencia
39. Sincronizar función
40. Anular de manera temporal los horarios de elevador
41. Activar alarma de intrusión
42. Desencadenar una alarma
43. Desencadenar una salida
44. Activar lectura

45. Desbloqueo de puertas explícitamente

F. La USP deberá permitir que un cronograma se asocie con una acción. Deberá activarse la acción solamente si es una acción adecuada para el período de tiempo actual.

2.34 Programas y tareas programadas de la USP

A. Programaciones

1. La USP deberá soportar la configuración y la administración de cronogramas complejos. Un usuario podrá agregar, borrar o modificar un horario si cuenta con los privilegios correspondientes.

2. La USP deberá ofrecer total flexibilidad y la capacidad de detallar cuando se crea un cronograma. El usuario deberá ser capaz de definir un cronograma en incrementos de 1 o 15 minutos.

3. Deberán soportarse programas diarios, mensuales, ordinales y específicos.

B. Tareas Programadas

1. La USP deberá soportar tareas programadas para video y ALPR.

2. Las tareas programadas deberán ejecutarse en un horario definido por el usuario en un día y hora específico. También deberá soportar tareas periódicas o recurrentes bajo un cronograma.

3. Las tareas programadas deberán soportar todas las acciones estándar disponibles dentro de la USP, como enviar un correo electrónico o enviar un informe por correo electrónico.

2.35 Macros y Scripts Personalizados de la USP

A. La USP deberá habilitar a los usuarios a automatizar y ampliar las funcionalidades del sistema a través del uso de macros o scripts personalizados para el control de acceso, video y ALPR.

B. Los macros personalizados deberán crearse con el Kit de Desarrollo de Software (SDK) de la USP.

C. Una macro deberé ejecutarse tanto de forma automática como manual.

D. Se deberá lanzar una macro en la UI de Monitoreo a través de acciones activas.

2.36 Mapas gráficos dinámicos (DGM) de la USP

A. La USP deberá soportar la funcionalidad de mapeo para el control de acceso, videovigilancia, detección de intrusión, ALPR y aplicaciones externas.

B. La USP deberá proporcionar una interfaz centrada en mapas con la habilidad de comando y control de todas las capacidades de la USP desde una interfaz de mapa de pantalla completa.

C. Deberá ser posible extender el mapa sobre todas las pantallas de la estación del cliente de la USP. En el escenario en donde el mapa se extiende sobre todas las pantallas de la estación del cliente de la USP, deberá ser posible navegar el mapa incluyendo panorámica y zoom, y los movimientos del mapa deberán estar sincronizados en todas las pantallas. La expansión del mapa en varias pantallas debe ofrecer las mismas capacidades de mando y control que la visualización en una sola pantalla.

D. Los DGM deberán soportar los siguientes formatos de archivos y protocolos para la importación de los fondos mapas:

1. PDF
2. JPG
3. PNG
4. Servicio de Mosaico de Mapas Web (WTMS, por sus siglas en inglés) y Servicio de Mapas Web (WMS, por sus siglas en inglés) definidos por el Open Geospatial Consortium (OGC)
5. BeNomad
6. AutoCAD (DWG y DXF)

E. El DGM deberá proporcionar los siguientes proveedores de mapas en línea para usar como fondo de mapa y proporcionar la habilidad de administrar su licencia de servicio, si se requiere una:

1. Google Map, aéreo, topografía (Con licencia)
2. Bing Map, aéreo, satélite, híbrido (Con licencia)
3. ESRI ArcGIS (con licencia)
4. Mapa aéreo OpenStreet (con licencia)
5. OVI híbrido

F. Deberá ser posible configurar un conjunto de mapas mixtos elaborados por GIS, proveedores en línea y archivos privados importados, y enlazarlos todos juntos.

G. Los DGM deberán proporcionar la habilidad de visualizar todas las entidades nativas de la USP, entre las que se incluyen:

1. Cámaras, corregir y PTZ
2. Puertas
3. Secuencias de cámaras
4. Áreas
5. Áreas de intrusión
6. Zonas de intrusión
7. Cámaras de reconocimiento de placas de matrícula

8. Entradas digitales
9. Salidas digitales
10. Intercomunicador
11. Alarmas
12. Macros
13. Patrollers de Patrullas Policiales

H. Los DGM deberán proporcionar la habilidad de dibujar y mostrar información sobre el mapa en la siguiente forma:

1. Formas vectoriales: líneas, rectángulos, polígonos y elipses
2. Fotos
3. Texto

I. Los DGM deberán proporcionar la habilidad de visualizar cualquier tipo de entidades de terceros integradas mediante un SDK. *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

J. Los DGM deberán proporcionar la habilidad de mostrar capas de información en el formato Keyhole Markup Language (KML).

K. El DGM deberá proporcionar la habilidad al operador de administrar capas de entidades visualizadas sobre el mapa, y ser capaz de encenderlas y apagarlas y cambiar el orden de superposición.

L. El DGM proporcionará la capacidad para importar capas de datos de uno o más servidores ESRI ArcGIS.

M. La DGM proporcionará a los operadores la capacidad para gestionar capas que son importadas de ESRI ArcGIS. Los usuarios podrán habilitar y deshabilitar las capas, al igual que clasificarlas.

N. El DGM ofrecerá una copia de seguridad y restauración de datos de mapas integrados para el fondo del mapa y las capas de entidades.

O. El DGM proporcionará la capacidad de importar configuración desde un archivo externo como:

1. Capa de AutoCAD para objetos
2. CSV, archivo de Excel

P. Los DGM deberán ofrecer capacidades de conmutación por error.

Q. Los DGM deberán ampliarse a varias miles de entidades sobre un solo mapa y cientos de mapas.

R. Los DGM deberán proporcionar un medio para actualizar el fondo de un mapa sin afectar la configuración del objeto de mapa.

S. Los DGM deberán ofrecer un diseñador de mapas gráficos fácil de usar para configurar los mapas.

T. Los DGM deberán proporcionar una navegación fácil e intuitiva que incluya:

   1. La habilidad para crear jerarquías de mapas para facilitar la navegación dentro y entre varios sitios y edificios.

   2. La habilidad para definir favoritos para una recuperación de posición recurrente.

   3. La posibilidad de crear vínculos entre mapas. Los enlaces de los mapas deberán permitir el vínculo desde un mapa a múltiples mapas que representan los pisos de un edificio. Mantener el nivel de zoom del mapa cuando se navegue por los pisos de un edificio

   4. Una experiencia común de usuario en relación a la navegación en el mapa para GIS y para mapas privados. *(Especificador, se requiere Plan Manager Advanced para GIS)*

U. Deberá ser posible monitorear el estado de entidades en el mapa. Deberá ser posible personalizar los íconos de cualquier entidad representada en el mapa.

V. Los DGM deberán ofrecer la habilidad de establecer de forma opcional una notificación de visualización gráfica de la detección de movimiento.

W. Los DGM deberán ofrecer una herramienta inteligente de selección para tener acceso al video. Al hacer clic en la ubicación que el usuario quiere ver, el DGM seleccionará de forma automática las cámaras que pueden ver esta ubicación y mover el PTZ hacia dicha ubicación. Esta herramienta inteligente de selección deberá tomar los obstáculos en consideración y no mostrar las cámaras que no pueden ver la ubicación debido a una pared.

X. Deberá ser posible seleccionar una ubicación dibujando una zona de interés en el DGM y visualizar todas las entidades que forman parte de dicha zona de interés a la vez.

Y. El usuario deberá ser capaz de seleccionar y visualizar el contenido de múltiples entidades de la USP sobre el mapa en las ventanas emergentes.

Z. El usuario deberá ser capaz de mover, redimensionar y fijar las ventanas emergentes de la entidad USP sobre el mapa.

AA. Deberá ser posible tener acceso a video en vivo y en modo de reproducción desde el mapa.

BB. Deberá ser posible monitorear desde el DGM todas las notificaciones de evento de entidades. Los usuarios podrán encender y apagar las notificaciones por entidad.

CC. Los DGM deberán ofrecer la habilidad de operar completamente la supervisión de alarma. Deberá ser posible:

   1. Centrar el mapa sobre entidades relacionadas con la alarma.

2. Visualizar las notificaciones de alarma sobre el mapa y tener acceso a los videos relacionados del mapa.
3. Activar y recibir alarmas.
4. Actuar sobre la alarma desde los DGM, incluyendo reconocimientos, reenvíos e investigación.
5. Visualizar que una alarma ocurrió en un mapa vinculado subyacente.

DD. Los DGM deberán proporcionar las siguientes capacidades de búsqueda:

1. Buscar y centrar por nombre de entidad.
2. Desde la Visualización de una entidad en la USP, ubique la entidad en el mapa y ofrezca la posibilidad de seleccionar otra cercana.
3. Por dirección postal, ciudad, punto de referencia, punto de interés (con licencia de geocodificador de Google, ESRI u otro proveedor)

EE. Cualquier actualización del contenido del mapa por parte de un administrador se enviará de forma inmediata y dinámica a todos los usuarios de DGM.

FF. El DGM deberá soportar el uso de mapas GIS, mapas privados o una combinación de ambos para el fondo del mapa. *(Especificador, se requiere Plan Manager Advanced para GIS).*

GG. El DGM deberá ser compatible con cualquier mapa compatible con GIS con el OGC y con WMTS y WMS de soporte. Esto incluye, más no se limita a, mapas ESRI. El DGM deberá permitir la selección de las capas GIS adecuadas. *(Especificador, se requiere Plan Manager Advanced para GIS).*

HH. Los DGM deberán proporcionar un diseñador de mapas intuitivo para el posicionamiento de la entidad sobre el mapa usando la opción arrastrar y colocar. Cualquier configuración deberá ser gráfica.

II. Será posible editar y configurar múltiples objetos del mapa a la vez.

JJ. Todas las modificaciones en el diseño del mapa se conectarán a un registro de auditoría.

KK. Estarán disponibles varias acciones dentro de los mapas para que se ejecuten con un doble clic simple e intuitivo, con un clic en el botón derecho o la funcionalidad de arrastrar y soltar. Los ejemplos de acciones disponibles a través de los mapas deberán incluir el desbloqueo de puertas y el reconocimiento de una alarma.

LL. Mediante las siguientes funcionalidades, los DGM deberán permitir la administración de alarmas de la USP desde el mapa *(Especificador, Plan Manager Standard y versiones superiores, se requiere licencia adicional)*:

1. Ubicar sobre el mapa entidades relacionadas con la alarma.
2. Mostrar entidades de la alarma con un icono específico, color, nivel de transparencia y velocidad de intermitencia.

3. Listar, seleccionar y ubicar alarmas.
4. Centrado automático del mapa sobre la alarma con mayor prioridad.
5. Manejar la alarma desde el mapa, incluyendo reconocimientos, reenvíos e investigaciones
6. Todos los contenedores del mapa, como puntos activos o enlaces de mapas, deberán reflejar el estado de la alarma de las entidades contenidas.

MM. Deberá ser posible agregar funcionalidad avanzada a objetos del mapa usando el SDK. Cualquier funcionalidad disponible mediante el SDK de la USP estará disponible dentro de los mapas. *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

NN. Los DGM deberán ofrecer la herramienta de lazo para:

1. Mostrar entidades en un sitio a través de una sola acción.
2. Activar una acción en todas las entidades de un sitio con un solo clic.
3. Editar múltiples entidades de un solo sitio en forma simultánea.

OO. Los DGM deberán permitir la visualización de las entidades de la USP seleccionadas desde el mapa sobre un monitor remoto (pared de video). *(Especificador: se requiere licencia adicional de Plan Manager Standard y versiones superiores).*

PP. El DGM deberá permitir realizar búsquedas en el mapa por nombre de la entidad.

QQ. Los DGM deberán permitir el uso de la información KML de mapas superpuestos tanto para mapas GIS como privados. Los objetos movibles deberán estar soportados mediante el uso de KML. *(Especificador: se requiere licencia adicional solo para Plan Manager Advanced)*

RR. El Contratista deberá proporcionar licencias para cada entidad que requiere ser mostrada en los mapas gráficos. *(Especificador, las licencias se venden en paquetes con base en la cantidad de entidades, especificar la licencia de un sitio o ilimitado después de 1,000 entidades)*

2.37 El Sistema de Administración de Evidencia Digital (DEMS, por sus siglas en inglés) de la USP (*Especificador, Genetec Clearance, se requiere suscripción por separado)*

A. La USP permitirá compartir videos exportados con terceros de forma electrónica.

B. La USP permitirá a los receptores revisar el video exportado de forma nativa desde un navegador, sin necesidad de instalar plugins de software o navegador.

C. Los videos exportados desde la USP incluirán el archivo original y la información de marca de tiempo, así como los metadatos fuente del sistema, la estación de trabajo y la cámara que pueden visualizarse desde el DEMS.

D. La USP permitirá crear un caso dentro del DEMS y asignar detalles asociados al incidente al exportar el video.

2.38 Auditoría y Registros de Actividades de Usuario de la USP (Registros)

A. La USP deberá soportar la generación de registros de auditoría. Los registros de auditoría deberán consistir de registros de adiciones, eliminaciones y modificaciones del operador/administrador,

B. Los registros de auditoría deberán generarse como informes. Deberán contar con la capacidad de rastrear cambios dentro de períodos de tiempo específicos. También deberá ser posible la consulta sobre usuarios específicos, cambios, entidades afectadas y períodos de tiempo.

C. Para los cambios de configuración de entidades, el informe de registros de auditoría deberá incluir información detallada sobre el valor antes y después de los cambios.

D. La USP deberá soportar la generación de registros de actividad del usuario. Los registros de actividad del usuario deberán consistir de registros de la actividad del operador en la USP como inicio de sesión, cámaras vistas, eventos ALPR, impresión de tarjetas de identificación, exportaciones de videos y otros.

E. El ACS deberá soportar las siguientes acciones sobre un informe de registros de auditoría y actividad: impresión y exportación de informes a un archivo PDF/Microsoft Excel/CSV.

2.39 Informes de Incidentes de la USP

A. Los informes de incidentes deberán permitir al operador de seguridad crear informes sobre incidentes que se presentaron durante un turno. Serán soportados los informes de incidentes relacionados con video y los incidentes relacionados con el control de acceso.

B. El operador será capaz de crear informes de incidentes independientes o informes de incidentes enlazados con las alarmas.

C. El operador deberá ser capaz de vincular secuencias múltiples de video a un incidente, tener acceso a los mismos, y cambiar la fecha u hora de las secuencias posteriormente.

D. Deberá ser posible crear una lista de categorías de Incidentes, etiquetar una categoría a un incidente, y filtrar la búsqueda con la categoría como parámetro.

E. Los informes de incidentes deberán permitir la creación de un formulario personalizado sobre el cual se incluya la información sobre un incidente.

F. Los informes de incidentes deberán permitir agregar entidades, eventos y alarmas para soportar las conclusiones del informe.

2.40 Ingestión de datos de USP

A. La USP deberá permitir la posibilidad de importar datos externos de fuentes externas para mejorar la unificación de las fuentes de datos dentro de la USP.

B. Cada fuente de datos se definirá mediante un conjunto de campos y tipos de campo que describen la fuente de datos. Los tipos de campo serán:

1. Cadena
2. Entero de 32 bits y 64 bits
3. Número de coma flotante
4. Booleano
5. Marca de tiempo
6. Binario (en un archivo o base 64)

C. La visualización de cada punto de datos de una fuente de datos será configurable para determinar qué campos de los datos deben mostrarse. La configuración de cada campo será:

1. Qué campos se muestran u ocultan
2. En qué orden se muestran los campos
3. Una etiqueta para especificar el nombre del campo (en formato clave:valor)
4. Una opción para especificar cómo mostrar el campo (valor de texto, Imagen, valor del portapapeles, hipervínculo a una página web, hipervínculo a una entidad en el sistema, archivo de sonido)

D. Debe haber un privilegio disponible para cada fuente de datos para permitir/denegar el acceso a usuarios y grupos de usuarios específicos de la USP.

E. Los datos ingeridos estarán disponibles en el sistema de informes de la USP.

F. Los datos ingeridos estarán disponibles para mostrarse en los Tableros de control de la USP.

2.41 Integración de terceros de USP

A. Integración de Microsoft Active Directory *(Especificador: se requiere licencia para Professional y versiones superiores)*

1. La USP deberá soportar una conexión directa a uno o varios servidores de Microsoft Active Directory mediante la(s) Función(es) del Active Directory. La integración del Active Directory deberá permitir la sincronización de información desde el servidor del Active Directory a la USP.
2. La integración del Active Directory deberá permitir la administración central de los usuarios, grupos de usuarios, tarjetahabientes y grupos de tarjetahabientes de la USP.
3. La USP deberá ser capaz de conectarse y sincronizar datos desde múltiples servidores de Active Directory (hasta 10).
4. La USP deberá soportar la sincronización de Grupos Universales del Active Directory al igual que la de grupos de seguridad que pertenecen a otros dominios dentro del mismo bosque.
5. La USP deberá soportar la encriptación del Microsoft Active Directory usando LDAP SSL.

6. Al estar habilitado, el Active Directory deberá administrar el inicio de sesión del usuario a las aplicaciones de la USP del cliente a través de las credenciales Windows del usuario. El inicio de sesión a la USP deberá utilizar características de administración y autenticación de contraseñas nativas del Active Directory.
7. Deberá ser posible sincronizar las siguientes entidades de la USP y su información desde el Active Directory con la USP:
    a. Usuarios (nombre de usuario, nombre y apellido, dirección de correo electrónico y demás)
    b. Grupos de usuarios (nombre del grupo de usuarios, descripción y dirección del correo electrónico del grupo)
    c. Atributos del Active Directory a los campos personalizados de la USP
8. Al estar habilitado, la adición, eliminación o suspensión de la cuenta Windows del usuario en el Active Directory deberá resultar en la creación, eliminación o deshabilitación de la cuenta de usuario equivalente en la USP.
9. Los métodos de sincronización admitidos para adiciones, modificaciones y eliminaciones de entidades sincronizadas deberán incluir en el primer inicio de sesión (solo usuarios), sincronización manual y sincronización programada.
10. La USP deberá admitir las conexiones de usuarios entre organizaciones independientes al conectarse a un proveedor de identidad mediante autenticación basada en notificaciones, como ADFS (Active Directory Federation Services), Azure Active Directory, otros proveedores de OpenID Connect y SAML2.

B. Integración de Detección de Intrusión: *(Especificador, Standard, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte el documento de Plugins Compatibles con Security Center)*

1. La USP se deberá integrar con los paneles de intrusión y dispositivos de terceros mediante un SDK de Intrusión. La Función del Intrusion Manager deberá manejar las comunicaciones con los paneles de intrusión. Las comunicaciones con los dispositivos de intrusión deberán ser sobre comunicaciones en serie y/o una red IP.
2. Deberá ser posible la integración con los paneles de intrusión fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.
3. La funcionalidad disponible mediante la integración de dispositivos de intrusión con la USP deberá incluir lo siguiente (en donde sea soportado por el panel de intrusión):
    a. Armar y desarmar dispositivos de intrusión (de forma manual, programada o después de un evento de la USP).
    b. Activación o accionamiento de salidas de dispositivos de intrusión.
    c. Visualización de eventos y alarmas de intrusión.

d. Vigilancia del estado, incluyendo el estado de armado de los dispositivos de intrusión.

e. Verificación por video de eventos y alarmas de intrusión con paneles de video.

f. Creación de zonas USP utilizando entradas de dispositivos de intrusión.

4. Los paneles de intrusión actualmente soportados incluyen:

a. Paneles Bosch de la serie G

b. Paneles DSC de la serie Power

c. Paneles DMP de la serie XR

d. Paneles Honeywell Galaxy Dimension y Flex

e. Vanderbilt SPC

f. UTC Advisor Master y Advanced

g. Bosch Map 5000

5. Dispositivos de intrusión adicionales compatibles:

a. BuyTime

b. Receptor de panel de alarmas

c. Southwest Microwave RPMII

C. Sistemas de Control de Acceso de Terceros: *(Especificador, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte la guía de Plugins compatibles con Security Center)*

1. La USP deberá integrarse con software de control de acceso de terceros a través del SDK. Las comunicaciones con software de control de acceso se producirán a través de una red IP y no deberían soportar tareas administrativas como la administración de tarjetahabientes.

2. Deberá ser posible la integración con software de control de acceso fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.

3. La funcionalidad disponible mediante la integración de software de control de acceso con la USP deberá incluir lo siguiente (en donde sea soportado por la solución de control de acceso):

a. Sincronice entidades de control de acceso y reciba estados y eventos asociados dentro de la USP, lo que incluye:

i. Derechos de acceso y tarjetahabientes

ii. Visitantes

iii. Lectores y puertas

iv. Alarmas

v. Entradas y salidas

b. Monitorear eventos de control de acceso.

c. Monitorear y reconocer alarmas de control de acceso.

d. Activar acciones y salidas en el software de control de acceso usando acciones activas y eventos a toma de acción.

e. Bloquear y desbloquear puertas en el software de control de acceso.

f. Verificación por video de eventos y alarmas de control de acceso.

g. Configurar eventos a toma de acción usando los eventos y las alarmas de control de acceso.

h. Generar informes de Security Center mediante el uso de datos de control de acceso.

i. Visualizar y monitorear estados de entidades de puertas en los mapas de la USP.

4. Entre los fabricantes de control de acceso actualmente compatibles, se encuentran los siguientes:

a. Tyco Softwarehouse CCURE

b. UTC Lenel Onguard

c. Amag Symmetry

d. Siemens Sipass

e. AssaAbloy ARX

D. Sistemas de Distribución de Destinos de Terceros: *(Especificador, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte la guía de Plugins compatibles con Security Center)*

1. La USP deberá integrarse con software de distribución de destinos (control de elevadores) de terceros a través del SDK. Las comunicaciones con el software de distribución de destinos se deberán realizar en una red IP.

2. Deberá ser posible la integración con software de distribución de destinos fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.

3. La funcionalidad disponible mediante la integración de software de distribución de destinos con la USP deberá incluir lo siguiente (en donde sea soportado por la solución de distribución de destinos):

a. Creación de entidades de la distribución de destinos y recepción de eventos y estados relacionados dentro de la USP, incluyendo lo siguiente:

i. Pisos y descansos

ii. Carros de elevadores (puertas delanteras y traseras) y quioscos

iii. Tarjetahabientes y credenciales (si corresponde)

b. Monitoreo de eventos de distribución de destinos.

c. Activación de acciones manuales de distribución.

d. Verificación por video de eventos de distribución de destinos.

e. Configuración de eventos a toma de acción mediante eventos de distribución de destinos.

f. Generación de informes de Security Center con los datos de la distribución de destinos.

g. Compatibilidad con varios lectores

i. Lectores internos de quioscos

ii. Lectores de la USP

h. Tipos de pasajeros y modos avanzados de quioscos.

4. Entre los fabricantes de distribución de destinos actualmente compatibles, se incluyen los siguientes:

a. Otis Compass

b. Thyssenkrupp

c. Schindler

d. MCE

E. Integración de Administración de Activos: *(Especificador, Professional y versiones superiores, se requiere licencia adicional)*

1. La USP se deberá integrar con los sistemas de administración de activos de terceros mediante la Función de Administración de Activos.

2. Las comunicaciones con las soluciones de la administración de activos deberán ser sobre una red IP (mediante comunicaciones de software).

3. La funcionalidad disponible mediante la integración de sistemas de administración de activos con la USP deberá incluir lo siguiente (en donde lo soporten los sistemas de administración de activos):

a. Sincronización de los activos del sistema de administración de activos con las entidades de activos de la USP.

b. Monitoreo en vivo de los eventos de actividades relacionadas con activos, eventos de los estados de salud y actividad (activo en línea, activo fuera de línea, movimientos de activo o baja batería).

c. Sincronización de alarmas de administración de activos con las alarmas del Security Center.

d. Visualización de video enlazado a actividades y alertas relacionadas con activos dentro de las tareas de generación de informes y monitoreo.

e. Reconocimiento de alarmas en Security Center el cual reconoce alertas en el sistema de administración de activos y viceversa.

f. Seguimiento en tiempo real de ubicaciones de activos por áreas.

g. Tarea de generación de informes de Inventario de Administración de Activos que muestra a detalle la ubicación actual (área) de un activo.

h. Tarea de generación de informes de Actividad de Activos que proporciona un resumen histórico de eventos y actividades relacionadas con activos.

4. Los sistemas de administración de activos actualmente compatibles incluyen:

a. Administración de claves Deister

b. Morsewatchmans

c. TRAKA

F. Integraciones Adicionales de Terceros:

1. La USP deberá soportar enfoques múltiples para la integración de sistemas de terceros. Estas deberán incluir: Kits de Desarrollo de Software (SDK), SDK de Servicio de Web basado en REST, SDK de Servicio RTSP, entre otros. *(Especificador, Professional y versiones superiores, se requiere licencia y paquete SDK)*

2. La arquitectura de la USP deberá soportar la adición de nuevas conexiones para adaptarse a la integración de sistemas de terceros, por ejemplo: *(Especificador: consulte el sitio web para ver cómo se otorgan las licencias; para obtener una lista actualizada de las integraciones de terceros, consulte la guía de plugins compatibles)*

a. Video analíticas

b. Sistemas de video de terceros

c. Sistemas de control de acceso de terceros

d. Integraciones de ALPR con estaciones de pago, proveedores de permisos, proveedores de pagos por teléfono y vendedores de boletos

e. Sistemas de administración de edificios

f. Ecosistema de Control de Acceso (como ID Scanner, sincronización de tarjetas, Guardtour y Morpho Biometrics)

g. Monitoreo de transacciones (POS, escaneo de códigos de barras y cajeros automáticos)

h. IoT Industrial (Modbus, BACnet, OPC, SNMP)

i. Industrial Protocol Interface (BACnet, Modbus)

j. Pared de video (Barco, Eizo)

k. Sistemas de administración de recursos humanos (HRMS)

l. Integración de Drones Autónomos

m. Teclas Inteligentes (Salto SVN, Medeco XT, CLIQ)

n. Detección de Disparos (Shot Spotter, Guardian GunShot)

o. Libro de Registro Dinámico

p. Plataforma de Reconocimiento Facial

q. Servicios de Localización en Tiempo Real - RTLS (HID)

2.42 Kit de desarrollo de software (SDK) de la USP

A. Un SDK de la USP deberá estar disponible para soportar el desarrollo personalizado para la plataforma.

B. El SDK deberá incluir funcionalidades específicas de los sistemas embebidos de reconocimiento automático de placas de matrícula (ALPR), control de acceso (ACS) y videos (VMS).

C. La integración con aplicaciones y bases de datos externas deberá ser posible con el SDK.

D. El SDK deberá permitir a los usuarios finales desarrollar nuevas funcionalidades (interfaz de usuario, aplicaciones o servicios independientes) para enlazar la USP a sistemas y aplicaciones empresariales de terceros como Sistemas para Uso de Emblemas, Sistemas de Administración de Recursos Humanos (HRMS), y sistemas de Planificación de Recursos Empresariales (ERP).

E. El SDK deberá basarse en la plataforma .NET.

F. El SDK deberá soportar actualizaciones dinámicas y transaccionales a la configuración de la USP. También deberá soportar el cambio de notificación de la configuración de entidad de la USP.

G. El SDK deberá proporcionar una lista completa de las funciones de programación para ver y/o configurar entidades básicas como lo son: usuarios y grupos de usuarios, alarmas, eventos personalizados, cronogramas. etc.

H. El SDK deberá proporcionar una lista completa de funciones de programación para ver y configurar el ACS, el VMS y el ALPR.

I. El SDK deberá proporcionar una lista completa de funciones de programación para ver y configurar la mayoría de las entidades ACS como: tarjetahabientes, grupos de tarjetahabientes, visitantes, credenciales, reglas de acceso (solo modificaciones) y campos personalizados.

J. El SDK deberá ser capaz de recibir eventos en tiempo real desde las siguientes entidades de la USP: usuarios y grupos de usuarios, áreas, zonas, cámaras, unidades de videos, puertas, controladores de puerta (unidades), elevadores, tarjetahabientes, grupos de tarjetahabientes y credenciales.

K. El SDK deberá ser capaz de consultar el historial de eventos para áreas, cámaras, zonas, alarmas, tarjetahabientes, credenciales, visitantes, puertas, eventos de

lectura de consultas de placa de matrícula, eventos de aciertos de placas de matrícula automotriz, generar un informe de aciertos de placa de matrícula , generar un informe de lecturas de placa de matrícula.

L. El SDK deberá soportar las siguientes funciones de alarma: visualización de alarmas en tiempo real, reconocimiento de alarmas, cambiar prioridades y cambiar destinatario.

Parte 3 - Ejecución

3.01 Garantía

A. El producto deberá desarrollarse en todos los aspectos materiales de acuerdo con el manual del usuario adjunto, y los medios en donde resida el Software del Producto estarán libre de defectos en material y mano de obra bajo uso normal. Los defectos de software están cubiertos mediante Lanzamiento de Servicios y Actualizaciones Acumulativas las cuales están disponibles por un 1 año a partir de la fecha de la compra del software.

B. La garantía prolongada, hasta por 5 años, deberá estar disponible mediante la compra del servicio de asistencia de Genetec, el cual incluye los siguientes servicios adicionales además de la garantía estándar:

1. Acceso a soporte telefónico y chat en línea para asistencia técnica.
2. Administración de caso en línea
3. System Availability Monitor en línea
4. Acceso a Actualizaciones de Versiones Importantes y Secundarias
5. Soporte de localizador 24/7 y especialistas dedicados de soporte *(Prescriptor, costo adicional)*

3.02 Puesta en marcha del sistema y servicios de integración *(Especificador, este es un cobro diario más viáticos, revisar Genetec Inc. para ver el número recomendado de días a especificar)*

A. Requisitos Generales:

1. El contratista deberá ocupar los servicios del integrador de la USP para asistir en la administración de la integración de la USP en el sitio del usuario final en proyectos que involucren:

a. Varios contratistas o subcontratistas serán responsables por la integración de la USP en varios sitios del cliente en diferentes zonas geográficas.

b. Las instalaciones empresariales complejas que involucran funcionalidades avanzadas (como la característica de Federation™, conmutaciones por error y plugins), sistemas múltiples (como control de acceso, videos y ALPR) o integraciones de terceros.

c. El amplio uso de soluciones/plugins personalizados desarrollados por el integrador que se integrarán en la USP.

2. Los servicios del integrador de la USP deberán incluir la Administración de la Integración y Configuración y Puesta en Marcha del Sistema.

B. Servicio de Administración de Implementación:

1. El servicio de Administración de Integración del integrador deberá incluir un Gerente de Proyecto que actúa como el único punto de contacto para todas las comunicaciones entre el contratista y la organización del proveedor quién será el responsable de:

a. Llevar a cabo la Evaluación de Riesgo del impacto sobre posibles factores de riesgo en el funcionamiento de la USP del integrador.

b. Proporcionar un plan de proyecto para la integración de la USP del integrador.

c. Administrar el desarrollo e implementación de los componentes de la solución personalizada que se integrarán a la USP del proveedor (si corresponde).

d. Proporcionar un ámbito del trabajo que indique en detalle los servicios ofrecidos por el proveedor para asistir en la implementación de la USP del integrador.

e. Coordinar y programar los servicios en campo del proveedor con el contratista para asistir en la implementación de la USP del proveedor.

f. Proporcionar actualizaciones regulares del estado del proyecto al contratista en relación a la implementación de las soluciones personalizadas (si corresponde) y la implementación de la USP del proveedor.

C. Servicio de Arquitecto de Soluciones:

1. El servicio de Arquitecto de Soluciones del proveedor deberá incluir un ingeniero de arquitectura de soluciones que actúe como único punto de contacto técnico durante la implementación de la USP y que será responsable de lo siguiente:

a. Asistir al contratista/subcontratista con el diseño y la arquitectura de la USP del proveedor.

b. Llevar a cabo actividades de consulta técnica que podrían incluir análisis de deficiencias/ajustes, revisiones de diseño del sistema, evaluaciones de compatibilidad de dispositivos, revisiones de diseño funcional y técnico, así como revisiones de rendimiento de la USP del proveedor.

c. Realizar una evaluación del sistema y garantizar el cumplimiento de las mejores prácticas de la USP del proveedor.

d. Proporcionar una estrategia de migración y actualización para la USP del proveedor según corresponda.

e. Proporcionar documentación con relación a la arquitectura del sistema, el diseño del sistema, las especificaciones de hardware y los requisitos de compatibilidad, los cálculos del ancho de banda de las cámaras y las mejores prácticas con respecto a la USP del proveedor.

D. Servicio de Configuración y Puesta en Marcha de Sistemas:

1. La Configuración del Sistema y el Servicio de Puerta en Marcha del proveedor deberá incluir un Ingeniero de Campo quien será responsable por:

a. Asistir a los técnicos en el lugar/remotos del contratista o subcontratista con la configuración y puesta en marcha de la USP del proveedor en el sitio del cliente.

b. Llevar a cabo una prueba de la USP después de la instalación del sistema usando escenarios del operador reales para asegurar un desempeño óptimo del sistema.

c. Proporcionar al contratista con un Informe de Servicio que indique con detalle las tareas realizadas durante la integración de la USP en el sitio del cliente, al igual que recomendaciones para mejorar el desempeño de la USP que deben ser implementadas por el contratista.

d. Proporcionar una transferencia de conocimiento de la USP del proveedor al contratista después de la implementación de la USP en el sitio del cliente.

3.03 Capacitación del Fabricante para el Operador Usuario Final *(Especificador: Este es un cargo de medio día más gastos)*

A. El contratista deberá contratar los servicios del proveedor de la USP para asistir en la capacitación del usuario final de la USP en el sitio final del usuario.

Fin de Sección

Sección 28 51 00 – Administración y Presentación de Información

Parte 1 - Información General

1.01 Trabajo relacionado

A. División 14 - Requisitos Generales para Elevadores

B. Sección 28 13 00 – Sistema Electrónico de Control de Acceso

C. Sección 28 23 00 – Videovigilancia

1.02 Definiciones

A. ACS - Sistema de Control de Acceso

B. CSA - Aplicación de Software del Cliente

C. DGM - Mapas Gráficos Dinámicos

D. DVS - Servidor Digital de Video

E. CDMS – Sistema colaborativo de administración de decisiones

F. ALPR – Reconocimiento Automático de Placas de Matrícula

G. SDK - Kit de Desarrollo del Software

H. SMA - Contrato de Mantenimiento de Software

I. SSM - Módulo de Software del Servidor

J. UI - Interfaz de Usuario

K. USP - Plataforma Unificada de Seguridad

L. USW - Cliente Web Unificado

M. VMS - Sistema de Administración de Videos

1.03 Requisitos

A. El programador del sistema deberá haber asistido a la capacitación del fabricante y obtenido la Certificación Técnica en Security Center - Omnicast™ de Genetec™.

B. Como opción, el programador del sistema deberá haber asistido a la capacitación del fabricante y obtenido la Certificación Técnica en Security Center - Enterprise de Genetec.

C. El programador del sistema deberá ser un Socio de Negocios Certificado Genetec con el siguiente nivel de preparación: *(Especificador: seleccione una de las siguientes opciones)*

1. Socio de Negocios Certificado o superior

2. Socio de Negocios Élite o superior
3. Socio de Negocios Élite Unificado

D. El programador del sistema deberá presentar comprobante de las certificaciones.

Parte 2 - Productos

2.01 Requisitos generales

A. El CDMS debe incorporarse de manera transparente en la Plataforma Unificada de Seguridad (USP).

B. El CDMS deberá basarse sobre una verdadera arquitectura abierta que deberá permitir el uso de estaciones de trabajo y hardware de servidores sin derechos de propiedad intelectual, infraestructura de red sin derechos de propiedad intelectual, y almacenamiento sin derechos de propiedad intelectual.

C. El CDMS debe ofrecer un juego operacional de herramientas íntegro y ampliable que permita el monitoreo en tiempo real y la administración de situaciones, al igual que funciones de análisis después de eventos.

D. El CDMS debe proporcionarlo el mismo fabricante como el núcleo de la USP y deberá interactuar de forma nativa con todos los componentes de la USP, lo que incluye, entre otros, VMS, ACS, comunicación, intrusión, plugins y accesorios.

E. La USP y el CDMS deben ser compatibles con futuros productos de manera que la actualización de uno no evite el uso del otro.

F. El CDMS debe ser compatible a la perfección con la USP y con cualquiera de sus componentes.

G. El CDMS deberá ofrecer las siguientes herramientas operacionales:

1. Administración de incidentes
2. Administración de documentos
3. Motor de reglas
4. Flujo de trabajo de automatización
5. Procedimientos estándar de operación
6. Interfaz del operador para el monitoreo de incidentes
7. Informes de incidentes

H. El CDMS debe proporcionar información de la situación al operador con un enfoque centrado en mapa y un resumen general detallado de los datos del incidente, en donde se combina el historial, los comentarios del operador, los registros de flujo de trabajo y acciones del operador, los procedimientos estándar de operación, el video pertinente en vivo y en modo de reproducción, y una secuencia agregada de eventos del incidente. La agregación de eventos tendrá la opción de basarse en las entidades en sí o en áreas designadas según la categoría.

I. El CDMS deber ser ampliable con el fin de soportar un flujo medio continuo de hasta 600 eventos por segundo, con irrupciones temporales de 5000 eventos por segundo. Debe ser capaz de enviar un mínimo de 20 incidentes por segundo y ejecutar los flujos de trabajo de automatización asociados.

J. La arquitectura del CDMS debe ser sumamente fiable con cero puntos de falla individuales. Los servidores del CDMS deben contar con la capacidad de conmutación por error con menos de 1 minuto de tiempo de inactividad y una garantía de una pérdida de eventos e incidentes de cero. No requerirá ninguna acción por parte del usuario en el caso de una falla del servidor.

K. La comunicación entre componentes del CDMS deberá ser cifrada, robusta y confiable.

L. El CDMS debe ofrecer un SDK para personalizar el activador de incidente, las condiciones de cierre del incidente, las actividades del flujo de trabajo de automatización, los datos del incidente y la visualización de los detalles del incidente. También será posible diseñar widgets personalizados dentro de la interfaz de usuario de CDMS.

M. El CDMS debe ofrecer una API estándar para activar y distribuir incidentes; obtener las configuraciones de los incidentes; obtener detalles de los incidentes, incluido el contenido de los procedimientos estándar de operación; modificar los estados, las prioridades, las descripciones, las ubicaciones y los tipos de incidentes; vincular incidentes; configurar las identificaciones externas de los incidentes, consultar el historial de un incidente.

N. La API estándar debe proporcionar un mecanismo de notificación para suscribirse para recibir actualizaciones sobre incidentes

O. Cualquiera de los dispositivos o características que ya cuentan con licencia en la USP no requerirán licencias adicionales para trabajar dentro del CDMS.

P. El CDMS deberá permitir una configuración basada en el operador de los usuarios del CDMS. Los privilegios con base en la función son heredados de los privilegios de la USP.

Q. El CDMS debe registrar todos los cambios de la configuración en un registro de auditoría con las configuraciones previas y posteriores.

R. El CDMS registrará todas las actividades del usuario que se ejecutan durante el tiempo en que un incidente está activo.

S. El CDMS debe proporcionar la capacidad de copiar la configuración de un incidente de manera parcial o total a uno o varios tipos de incidentes.

T. El CDMS debe proporcionar la capacidad de configurar incidentes en un modo de prueba que permitiría que los usuarios con el privilegio apropiado validen distintos parámetros antes de activar la configuración del incidente.

2.02 Interfaz de Usuario Gráfica del CDMS

A. El CDMS debe ofrecer una GUI sencilla e intuitiva dentro de la GUI de la USP. Las herramientas del CDMS deben ser una serie de tareas adicionales.

B. El CDMS debe proporcionar tareas a la USP para:

1. Monitoreo de incidentes
2. Visualización de detalles del incidente
3. Generación de informes de incidentes
4. Administración de incidentes

C. El monitoreo de incidentes debe proporcionar:

1. Una lista de los incidentes actuales. La lista de incidentes actuales se debe poder adaptar a la función y necesidades del operador, con herramientas como el agrupamiento de incidentes en niveles múltiples, y el filtrado y búsqueda avanzada.
2. Un Mapa Gráfico Dinámico que muestra las ubicaciones del incidente y ofrece una percepción situacional completa de la seguridad en un área geográfica.
3. Un Panel Detallado de Incidente con toda la información relacionada para el incidente seleccionado:
    a. Resumen General
    b. Actividades más recientes
    c. Incidentes relacionados
    d. Entidades relacionadas
    e. Documentos relacionados
    f. Vistas personalizadas (SDK)
4. Acceso a todos los controles disponibles en la USP.

D. El CDMS debe estar diseñado para el uso óptimo con estaciones de trabajo con pantallas múltiples, permitiendo una combinación de lista de incidentes, el mapa gráfico dinámico, y los detalles del incidente a visualizarse en cada pantalla. La GUI del CDMS debe contar con la capacidad de sincronizar todas las pantallas de manera que la selección de un incidente enfoque de forma automática todas las otras pantallas con los datos del incidente. Las pantallas deben tener la capacidad de estar sincronizadas por uno o cualquier combinación de ajustes de selección de incidentes, filtro de visualización o vista de columna.

E. El Mapa Gráfico Dinámico debe ofrecer información sobre herramientas con un resumen del incidente al seleccionar un incidente en el mapa. Incidentes múltiples en la misma ubicación se agruparán en un objeto en el mapa. El grupo mostrará el incidente con el mayor nivel de prioridad y el número de incidentes en el grupo.

También debe ser posible visualizar una lista de todos los incidentes dentro del grupo.

F. Debe ser posible configurar un mapa para visualizar todos los incidentes de todos los mapas en una sola vista con base en sus coordenadas GPS relativas.

G. La tarea de Monitoreo de Incidentes se puede configurar para visualizar la lista de incidentes, el mapa de incidentes, los detalles del incidente, o cualquier combinación de estos elementos.

H. La lista de incidentes debe permitir al operador agrupar el incidente por:

1. Categoría de incidente
2. Tipo de incidente
3. Prioridad del incidente
4. Estado del incidente
5. Ubicación del incidente
6. Propietario del incidente
7. Cualquier atributo personal del incidente

I. Debe ser posible guardar la interfaz del operador, y la configuración de la GUI debe permanecer igual después que un operador inicie o cierre una sesión.

J. La GUI del CDMS debe ofrecer herramientas avanzadas para auxiliar a los operadores a enfocarse en una misión. El filtro se puede aplicar a la tarea actual o de forma simultánea a todas las tareas.

K. La GUI del CDMS debe proporcionar un área de visualización expansible para editar el diagrama asociado con un procedimiento operativo estándar dinámico.

2.03 Administración de Incidente del CDMS

A. El CDMS debe ser la interfaz que visualiza todas las situaciones como incidentes.

B. La administración de incidentes del CDMS debe ofrecer la habilidad de activar incidentes de forma manual o automática con base en una correlación de eventos.

C. Un incidente debe ser una descripción holística de la situación y soportar los siguientes atributos:

1. Visual:
   a. Color.
   b. Icono. La administración de incidente debe ofrecer la capacidad de personalizar tipos de incidentes usando un juego de iconos importados.
2. Sonido.
3. Categoría de incidente. La categoría de incidente debe permitir al operador organizar tipos de incidentes en un árbol lógico.

4. Una ubicación. La ubicación puede ser una entidad (cámara, puerta, zona, área) o una coordenada geográfica.
5. Un nivel de prioridad.
6. Una descripción.
7. Estados.
8. Procedimientos estándar de operación.
9. Historial de actividades.
10. Entidades adjuntas. Las entidades relacionadas a la fuente de eventos que activan el incidente deben asociarse de forma automática al incidente.
11. Documentos adjuntos. Documentos y URL que proporcionan más información u orientación sobre el incidente y su administración.
12. Un horario durante el cual será válido la activación automática de un incidente por parte del sistema.

D. El CDMS debe permitir al operador configurar hasta 255 niveles de prioridad, se pueden configurar para respetar la convención de nombre de la operación.

E. El CDMS debe ofrecer una máquina de estado configurable que definirá la transición de estados. Por ejemplo, usted puede configurar el estado E para que esté disponible solo si el incidente está en el estado C o D. Por lo tanto, si el incidente se encuentra en el estado A o B, el estado E no está disponible.

F. Los estados del incidente deben poder configurarse de tal forma que solo usuarios específicos cuenten con el privilegio para cambiar el estado del incidente a un estado en particular.

G. La administración de incidente debe proporcionar una posesión de administración de incidente. Debe ser posible solicitar o liberar de forma explícita la posesión de un incidente. La posesión de un incidente debe proporcionarse de forma inmediata a un operador que empieza a trabajar sobre un incidente.

H. Un supervisor debe ser capaz de visualizar todos los incidentes que están bajo su supervisión y ver la propiedad de cada incidente. En la misma visualización el supervisor debe recibir información en tiempo real sobre quién está monitoreando actualmente un incidente.

I. El CDMS deberá notificar al supervisor cuando un operador omita un paso en el procedimiento operativo estándar (SOP, por sus siglas en inglés).

J. El CDMS deberá ofrecer la capacidad de solicitar el consentimiento del propietario actual antes de tomar propiedad de un incidente.

K. El CDMS debe proporcionar una manera de definir incidentes colaborativos para permitir que varios operadores trabajen con el mismo incidente.

L. Debe ser posible configurar diferentes SOP y flujos de trabajo de automatización para distintos destinatarios de un incidente colaborativo.

M. Debe ser posible cambiar el tipo de incidente, de manera manual o automática.

N. El CDMS permitirá la exportación del tipo de incidente y la configuración de la categoría con íconos personalizados. El CDMS debe permitir que se importe la configuración exportada.

O. El CDMS debe permitir la exportación de todos los subincidentes adjuntos a un incidente colaborativo o todos los incidentes creados a partir de un incidente maestro, desde el flujo de trabajo de automatización o cambiando el tipo de incidente de forma manual.

P. Para cada incidente, debe ser posible abrir los detalles del incidente o configurar el incidente para que abra los detalles de forma automática. Los detalles del incidente se abrirán en una pantalla configurable y proporcionar, con base en la configuración del tipo de incidente, la siguiente información:

    1. Un diagrama de todo el video en vivo y en modo de reproducción relacionado con el incidente, incluyendo la cámara asociada a la fuente y la ubicación del incidente, al igual que el mapa local centrado sobre la ubicación del incidente.
    2. Historial del incidente, incluido:
        a. Todos los eventos relacionados con el incidente
        b. Actividades de flujo de trabajo de automatización del sistema
        c. Acciones del operador para el incidente
        d. Comentarios sobre el incidente

Q. Los operadores deben ser capaces de realizar las siguientes acciones:

    1. Cambiar el estado del incidente.
    2. Reenviar el incidente.
    3. Transferir el incidente.
    4. Editar el incidente:
        a. Cambiar la descripción
        b. Cambiar el nivel de prioridad
        c. Liberar la posesión
    5. Agregar entidades adicionales al incidente.
    6. Vincular incidentes relacionados.
    7. Adjuntar un documento como enlace URL al incidente.

R. Distribución de incidente:

    1. El CDMS debe proporcionar la capacidad de distribuir un incidente a un usuario o grupo de usuarios. La distribución de un incidente a un número restringido de usuarios asegurará el acceso a la información.

a. El envío de incidentes tendrá la capacidad de realizarse al grupo de usuarios seleccionado según el orden de inicio de sesión (round robin). Si todos los usuarios están desconectados, el envío de incidentes sigue el formato del envío de incidentes ordinario y se envía a todos los miembros del grupo de usuarios seleccionado.

2. El CDMS permitirá la distribución de tareas específicas (administradas como subincidentes) que están asociadas a un incidente único, a equipos humanos distintos. Los procedimientos se pueden llevar a cabo en paralelo.
3. Los supervisores de incidentes podrán ver todos los sub-incidentes asociados con un incidente principal.
4. El CDMS debe administrar la distribución de incidentes por:
   a. Tipo de incidente
   b. Calendario
   c. Ubicación. Donde debe ser posible definir la ubicación por:
      i. Entidad
      ii. Área (grupo de entidades)
5. Debe ser posible activar una nueva distribución durante el transcurso de un incidente:
   a. Por una acción del operador en la GUI. El usuario debe tener la opción de:
      i. Transferir el incidente, es decir, el incidente ya no se encuentra en la lista de incidentes del usuario. El usuario cuenta con la opción de solicitar confirmación de la transferencia.
      ii. Reenvío de un incidente, es decir, el incidente seguirá estando en la lista de incidentes del usuario y el usuario sigue siendo un destinatario de este incidente.
      iii. Solicitud para apropiarse del incidente.
      iv. Elevar un incidente
6. Se podrán definir perfiles para garantizar la distribución adecuada de los incidentes activos entre los operadores que estén conectados al sistema y filtrar incidentes por tipo y lugar de ocurrencia.
   a. El sistema debe tener la capacidad de asignar perfiles de administración de incidentes, de manera automática, a usuarios cuando inician sesión.
   b. Los perfiles solo se asignarán a los usuarios que hayan iniciado sesión en el sistema.
   c. Los perfiles serán asignados por el sistema o por usuarios con los privilegios requeridos.
   d. Se podrá asignar un perfil a usuarios o grupos de usuarios específicos.
   e. Se podrán especificar tipos de incidentes y ubicaciones asociados con un perfil.

f. Cuando se asigna un perfil a un operador, el sistema debe ocultar todos los incidentes que no especifica el perfil desde la vista del operador.

g. Se podrán asignar múltiples perfiles a un operador. Cuando se asignan múltiples perfiles, el operador debe visualizar los incidentes especificados por todos los perfiles asignados.

h. Se podrá activar o desactivar un perfil existente.

i. Las modificaciones a la configuración del perfil deben ser rastreables en un informe y este informe se debe poder exportar.

j. La carga debe equilibrarse de acuerdo con la disponibilidad de los operadores y sus privilegios

k. Los incidentes deben transferirse de forma automática a destinatarios autorizados si no hay operadores en línea para un perfil determinado

S. Capacidad de definir recordatorios:

a. Los recordatorios para el operador deben configurarse de acuerdo con un horario.

b. Los recordatorios mostrarán mensajes específicos de texto para el operador. Además, los recordatorios se deben poder agregar de forma automática a través del flujo de trabajo de automatización del incidente.

c. Aparece un mensaje de advertencia cuando se resuelve un incidente con un recordatorio activo.

2.04 Informe de incidentes del CDMS

A. El CDMS debe ofrecer una tarea para administrar y generar informes. La habilidad para ejecutar un informe es un privilegio de usuario.

B. Deberá ser posible solicitar el filtrado del historial de incidentes por:

1. Tipo de incidente

2. Estado del incidente

3. Ubicación

4. Prioridad

5. Rango de activador de tiempo

6. Propietario del incidente

7. Descripción

C. El resultado de una consulta de informes debe proporcionar una lista de incidentes al igual que una imagen visual de las ubicaciones de estos incidentes sobre el mapa. Cuando se reporten más de un incidente en una ubicación, la GUI agrupará estos incidentes en el mapa.

D. Al seleccionar un incidente de la lista o en el mapa se visualizarán los detalles del incidente que contienen la misma información disponible en la tarea de Monitoreo de Incidente.

E. Para incidentes cercanos, el incidente debe estar en modo de solo lectura con la excepción para agregar vínculos a incidentes relacionados.

F. La tarea Informes también debe reportar el registro de actividad del usuario de la USP desde la hora en que el operador era el propietario del incidente y lo estaba monitoreando, a manera de proporcionar una visualización de todas las acciones tomadas para la resolución de este incidente.

G. Debe ser posible exportar todos los datos incluidos en los detalles del incidente. La exportación del incidente debe incluir como mínimo:

    1. Un resumen general del incidente, el propietario, descripción, ID, prioridad, ubicación y GPS.
    2. El registro de actividad, incluido comentarios, eventos y todas las acciones tomadas por el sistema o por el operador durante la resolución de este incidente.
    3. Entidades y documentos relacionados.
    4. Instantánea del mapa. Debe ser una opción para el operador durante la exportación.
    5. Instantánea de la cámara al momento de los eventos agregados. Debe ser una opción para el operador durante la exportación.
    6. Secuencia de video del activador de evento.

H. El CDMS debe ofrecer todos los informes en un formato de presentación visual (como gráficos circulares, líneas, columnas y filas).

I. El CDMS deberá soportar los siguientes formatos de informes:

    1. • HTML
    2. PDF
    3. XML
    4. Formatos personalizados

J. Se exigirán privilegios específicos para modificar incidentes desde la interfaz de informes.

K. Se podrá generar un informe sobre la base de los perfiles definidos para el CDMS.

L. La capacidad del período de retención del informe de incidentes debe ser personalizable (de 1 a 9999 días o indefinidamente).

    1. El informe del perfil se debe poder exportar e imprimir.
    2. Los informes de perfiles deben permitir aplicar filtros sobre el identificador del perfil, iniciadores, destinatario y hora de modificación.

3. Las columnas de los informes de perfiles deben poder configurarse.

2.05 Administración Dinámica de Documentos del CDMS

A. La plataforma del CDMS debe proporcionar la habilidad de indexar documentos de forma dinámica a un incidente de manera de mejorar la eficiencia del acceso a la información por parte de un operador.

B. Se debe poder adjuntar un documento de forma automática a un incidente si las propiedades del documento concuerdan con las propiedades del incidente. Se debe contar con las siguientes propiedades:

1. Tipo de incidente
2. Calendario
3. Ubicación. La ubicación puede ser una entidad o un área.
4. Usuario o grupo de usuarios del operador monitoreando el incidente.

C. El CDMS debe ofrecer la habilidad de vincular un documento de forma automática a un paso en un procedimiento estándar de operación.

D. La Gestión de Documentos proporcionará un sistema de archivos para almacenar todos los documentos, así como las URL de los documentos para el uso de sistemas de archivos de terceros.

2.06 Motor de reglas del CDMS

A. El CDMS debe ofrecer un Motor de Reglas avanzado para correlacionar eventos y activadores de incidentes usando reglas booleanas.

B. La configuración del Motor de Reglas debe ser gráfica sin la necesidad de un guion.

C. El Motor de Reglas debe proporcionar la habilidad de configurar una secuencia de condiciones con AND y OR de manera que cuando coincida la secuencia se active un incidente.

D. La condición del Motor de Reglas debe permitir al usuario configurar:

1. Una lista de eventos desde diferentes ubicaciones o desde la misma ubicación con un operando OR entre los mismos.
2. El número de ocurrencias de cualquier evento seleccionado.
3. Un lapso máximo de tiempo durante el cual se debe validar la condición.
4. Un filtro para otros eventos en el sistema.

E. Deberá ser posible configurar una secuencia compleja de reglas aplicando la ocurrencia, el intervalo y el filtrado de eventos.

F. También debe ser posible hacer una secuencia de las reglas por adelantado e importarlas después al sistema.

2.07 Motor de Flujo de Trabajo de Automatización del CDMS

A. El CDMS deberá proporcionar un Motor de Flujo de Trabajo de Automatización para automatizar la respuesta a un tipo de incidente.

B. El flujo de trabajo de automatización debe ser altamente escalable y de clase empresarial, permitiendo la implementación de reglas empresariales complejas.

C. El CDMS debe proporcionar un diseñador gráfico de flujo de trabajo de automatización. No será necesaria una habilidad de secuencia para implementar un flujo de trabajo.

D. Debe ser posible definir un flujo de trabajo de automatización para cada tipo de incidente. El flujo de trabajo de automatización debe ser una serie de actividades que se ejecutan de forma secuencial.

E. Debe ser posible copiar y pegar una porción o todo el flujo de trabajo de automatización dentro de otro flujo de trabajo de automatización.

F. El flujo de trabajo de automatización soportará la ejecución de ramas paralelas.

G. El flujo de trabajo de automatización soportará actividades condicionales mediante escenarios de sentencia condicional.

H. Se podrá observar el estado de la puerta (bloqueada, desbloqueada, con seguridad, sin seguridad o abierta) para habilitar o deshabilitar acciones adicionales.

I. El Motor de Flujo de Trabajo de Automatización debe proporcionar las siguientes actividades:

1. Reconocer alarma
2. Agregar recordatorios
3. Eventos agregados
4. Zonas armadas
5. Cambio de colores de la pantalla
6. Cambio de descripciones de incidente
7. Cambio de estados de incidente
8. Cambio de tipos de incidente
9. Cambio de prioridades
10. Cierre de incidentes
11. Retrasar
12. Incidentes futuros
13. Transferencia de incidentes
14. Desarmado de zonas

15. Visualización de entidades
16. Distribución a
17. Exportar incidentes
18. Reproducción de sonidos
19. Comandos PTZ
20. Restablecimiento de conteo de personas en el área
21. Ejecutar una macro
22. Enviar un correo electrónico
23. Establecer un nivel de amenaza
24. Activación de alarmas
25. Activación de incidentes
26. Desbloqueo de puertas explícitamente
27. Espera de eventos
28. Espera de estados de incidente
29. Actividades personalizadas: construir sus propias actividades aprovechando el SDK y su interacción con Security Center y/o sistemas externos.
30. Reproducir un archivo MP3 o WAV a un sistema de anuncios públicos de Sipelia™.
31. Desencadenar una salida
32. Habilitar/Deshabilitar la transición del estado
33. Esperar a la prioridad del incidente

J. El Motor de Flujo de Trabajo de Automatización debe proporcionar una plataforma para crear actividades personalizadas que permitan la integración a un proceso empresarial global.

K. El Flujo de Trabajo de Automatización debe proporcionar una forma de tener acceso a información de contexto para las actividades de Correo y Macro.

2.08 Procedimiento Operativo Estándar del CDMS

A. El CDMS debe proporcionar orientación a los operadores en la forma de un procedimiento estándar de operación (SOP) para la respuesta ante un tipo de incidente.

B. El SOP debe ser interactivo y ofrecer una opción operador-reconocimiento-auditoría para cada paso del SOP.

C. El SOP debe ser dinámico y proporcionar la capacidad de adaptar los siguientes pasos de un procedimiento en función de las respuestas a pasos anteriores del procedimiento.

D. La configuración de la secuencia dinámica para el SOP se debe representar de forma visual a través de un diagrama de flujo.

E. La GUI del CDMS debe proporcionar la habilidad de saltarse un paso del SOP y volver a solicitar una justificación por saltarse dicho paso.

F. Debe ser posible configurar un SOP tanto de forma secuencial, requiriendo la validación para cada paso a manera de lograr acceso al siguiente paso, o bien, dejarse a la discreción del operador de ejecutar los pasos como una lista de verificación en un orden abierto.

G. El SOP debe ser configurable de manera que la validación de todos los pasos en el SOP sean obligatorios a manera de cerrar el incidente.

H. Cada paso debe, de forma opcional, estar asociado con un documento en la forma de un URL o un documento en un formato compatible (como Word, PDF o HTML).

I. El CDMS deberá hacer un seguimiento del tiempo dedicado a cada paso del SOP, así como del tiempo total transcurrido desde la respuesta inicial hasta la resolución.

J. El CDMS deberá proporcionar la capacidad de importar y exportar el SOP de manera individual como archivos CSV.

K. El CDMS deberá proporcionar la capacidad de configurar opciones estándar al definir pasos dinámicos del SOP.

L. El CDMS debe proporcionar la capacidad de configurar SOP Dinámicos (DSOP, por sus siglas en inglés) con una vista de árbol de decisiones.

M. El CDMS debe proporcionar la posibilidad de ejecutar acciones específicas en función de las respuestas del DSOP. Las respuestas deben proporcionarse a través de selecciones predefinidas o personalizadas. Las selecciones pueden hacerse con el ratón o accesos directos.

N. El CDMS debe proporcionar una GUI para configurar el DSOP y conectar los distintos pasos en función de la respuesta del operador. El CDMS debe proporcionar la capacidad de llamar a un dispositivo Sipelia™ al utilizar la integración de Sipelia™ desde el paso del SOP dinámico.

O. Se permitirá un retraso máximo para que un usuario inicie el procedimiento. Las acciones automáticas asociadas con este umbral de tiempo de respuesta deben ser configurables.

P. Se permitirá un retraso máximo para que un usuario complete el procedimiento. Las acciones automáticas asociadas con este umbral de tiempo de resolución deben ser configurables.

Q. Se asignará un tiempo mínimo para que un usuario complete el procedimiento. Cerrar el incidente antes de pasar este umbral de tiempo de resolución activará acciones automáticas.

R. Se mostrará un indicador visual cuando se exceda el tiempo de respuesta máximo o el tiempo de resolución máximo para el incidente.

2.09 Sistema del Control de Acceso Electrónico *(Especificador, seleccionar una de las siguientes opciones)*

A. La Administración y Presentación de Información debe estar unificada a la perfección con el Sistema de Control de Acceso especificado en la sección 28 13 00 dentro de la USP. Todas las características de control de acceso disponibles en la USP deben estar disponibles al software de la Administración y Presentación de Información.

B. La Administración y Presentación de Información debe estar unificada a la perfección con los plugins del Sistema de Control de Acceso de la USP. Todas las características de control de acceso disponibles en la USP deben estar disponibles al software de la Administración y Presentación de Información.

2.10 Sistema de Administración de Videos *(Especificador, seleccione una de las siguientes opciones)*

A. La Administración y Presentación de Información debe estar unificada a la perfección con el Sistema de Administración de Videos especificado en la sección 28 23 00 dentro de la USP. Todas las características de administración de videos disponibles en la USP deben estar disponibles al software de la Administración y Presentación de Información.

B. La Administración y Presentación de Información debe estar unificada a la perfección con los plugins del Sistema de Administración de Videos de la USP. Todas las características de administración de videos disponibles en la USP deben estar disponibles al software de la Administración y Presentación de Información.

2.11 Requisitos de la Interfaz de Usuario del Administrador del Servidor

A. El Administrador del Servidor se usará para configurar el SSM y la Función de Directory (configuración principal) y su(s) base(s) de datos para aplicar la licencia, y otros más.

B. El Administrador del Servidor será una aplicación basada en la Web. A través del Administrador del Servidor será posible tener acceso al SSM a lo largo de la red o de forma local en el servidor.

C. El acceso al Administrador del Servidor estará protegido a través de un nombre de inicio de sesión, contraseña y comunicaciones encriptadas.

D. El Administrador del Servidor deberá permitir al administrador (usuario) realizar las siguientes funciones:

1. Administrar la licencia del sistema.

2. Configurar las bases de datos y el servidor de la base de datos para la Función de Directory.
3. Activar/ Desactivar la Función de Directory
4. Respaldar manualmente la(s) base(s) de datos de la Función de Directory y/o restaurar la(s) base(s) de datos del servidor, al igual que configurar las copias de seguridad programadas de las bases de datos.
5. Definir las configuraciones de seguridad de las comunicaciones entre el cliente y el servidor.
6. Configurar el hardware de comunicaciones de la red, incluidos las direcciones y los puertos de conexión.

2.12 Requisitos Generales para Aplicaciones para Teléfonos Inteligentes y Tabletas

A. La USP deberá soportar aplicaciones móviles para diferentes dispositivos disponibles en el mercado. Las aplicaciones móviles deberán comunicarse con la USP a través de cualquier conexión wifi o conexión de red móvil.

B. Las aplicaciones móviles deberán comunicarse con la USP a través de una función del Mobile Server (MSR, por sus siglas en inglés). Toda comunicación entre las aplicaciones móviles y la MSR estará basada en el protocolo TCP/IP estándar y deberá usar la encriptación TLS con certificados digitales para proteger el canal de comunicación.

C. Los fabricantes de los dispositivos soportados incluyen (consultar las especificaciones de aplicaciones móviles para ver la lista de compatibilidad más reciente):

1. Dispositivos Apple con iOS 11 o posterior
2. Dispositivos con Android 6.0 o más reciente

D. Deberá ser posible descargar las aplicaciones móviles desde la tienda de aplicaciones Central (Apple iTunes App Store, Google Play).

E. Deberá ser posible enviar la configuración a los dispositivos móviles a través de una solución de administración de dispositivos móviles como VMWare Workspace One o Microsoft Intune.

F. Funcionalidades

1. Principales

a. Posibilidad de iniciar sesión / cerrar sesión en la USP utilizando un perfil de usuario autorizado del sistema.

b. Capacidad para admitir la autenticación pasiva de un proveedor de inicio de sesión única (proveedor de identidad Open ID Connect o SAML2)

c. Posibilidad de utilizar funciones biométricas (huella digital, identificación facial, etc.) para realizar la conexión al sistema.

d. Posibilidad de modificar la imagen o contraseña del usuario de la Mobile app.

e. Posibilidad de ver el Nivel de Amenaza actual del sistema.

f. Posibilidad de modificar el Nivel de Amenaza actual del sistema.

g. Posibilidad de ejecutar acciones activas configuradas en el perfil del usuario.

h. Posibilidad de ver entidades de la USP:

   i. Cámeras

   ii. Puertas

   iii. Cámaras ALPR

   iv. Plugins de Mosaicos Web

   v. Planos

   vi. Secuencias de Cámaras

   vii. Macros

   viii. Mapas (solo mapas geográficos) *(Especificador, se requiere licencia adicional, Plan Manager Advanced)*

i. Posibilidad de navegar por la vista jerárquica de las entidades del sistema y buscar entidades en el sistema.

2. Vídeo

   a. Posibilidad de ver video en vivo y grabado en las cámaras de la USP. Se podrán ver cuatro cámaras como máximo.

   b. Posibilidad de ver videos en formato nativo (H.264).

   c. Posibilidad de ver en paralelo video en vivo y grabado para una cámara específica.

   d. Posibilidad de utilizar zoom digital en las cámaras.

   e. Posibilidad de realizar acciones en las cámaras, como agregar un marcador, controlar un PTZ, controlar la función de iris/enfoque, guardar una instantánea e iniciar/detener una grabación.

   f. Posibilidad de ver planos de cámaras.

   g. Posibilidad de ver secuencias de cámaras.

   h. Posibilidad de ejecutar un informe de eventos de cámaras.

   i. Posibilidad de modificar la calidad de video de las cámaras que se muestran en la aplicación móvil.

   j. Posibilidad de usar la cámara del teléfono inteligente y transmitir una secuencia de video en vivo a una grabadora de video del sistema.

3. Control de Acceso

   a. Posibilidad de ver el estado de la puerta y de la cerradura de la puerta.

b. Posibilidad de realizar acciones en una puerta, como desbloquearla, cambiar el modo a modo de mantenimiento y anular el horario de desbloqueo.

4. Reconocimiento Automático de Placas de Matrícula

a. Posibilidad de ver eventos en vivo de una cámara ALPR.

b. Posibilidad de ver la imagen de lectura, la imagen contextual y todos los metadatos que captura la cámara ALPR

c. Posibilidad de ejecutar un informe de eventos ALPR.

d. Posibilidad de agregar una placa de matrícula a una lista activa del sistema.

5. Administración de alarmas

a. Posibilidad de recibir notificaciones push para notificar a los operadores móviles de la recepción de una alarma.

b. Posibilidad de ver todas las alarmas activas asignadas al operador móvil.

c. Posibilidad de realizar acciones en una alarma, como reconocer, reenviar o alternar el reconocimiento de una alarma activa.

d. Posibilidad de ver entidades vinculadas a la alarma.

6. Mapas *(Especificador, se requiere licencia adicional, Plan Manager Advanced)*

a. Posibilidad de ver mapas geográficos con entidades de la USP localizadas geográficamente en el mapa.

b. Posibilidad de ver cualquier entidad configurada en el mapa.

c. Posibilidad de buscar entidades o ubicaciones en el mapa.

G. Posibilidad de enviar un mensaje desde la interfaz del usuario de clientes a un operador móvil.

H. Posibilidad de enviar una secuencia de video en vivo o grabada desde la interfaz del cliente a un operador móvil.

I. Posibilidad de ver los operadores móviles que hayan habilitado el rastreo de ubicación en un mapa del sistema. La ubicación del operador móvil debería actualizarse en tiempo real. *(Especificador, Plan Manager Advanced, se requiere licencia adicional)*

2.13 Monitor de salud

A. La USP deberá monitorear el estado de salud del sistema, los eventos relacionados con los registros del estado de salud y calcular estadísticas.

B. Los servicios de la USP, funciones, agentes, unidades y aplicaciones de clientes activarán los eventos de los estados de salud.

C. La USP deberá llenar el Registro de Eventos Windows con eventos del estado de salud relacionados con las funciones de la USP, servicios y aplicaciones de clientes.

D. Una función exclusiva, la Función de Monitoreo del Estado de Salud, deberá realizar las siguientes acciones:

1. Monitorear el estado de la salud de todo el sistema y los eventos de registros.
2. Calcular estadísticas dentro de un marco de tiempo específico (horas, días, meses).
3. Calcular la disponibilidad para los clientes, servidores y unidades de videos/acceso/ALPR.

E. Una tarea de Monitoreo del Estado de Salud y una tarea de generación de informes del Historial del Estado de Salud deberá estar disponible para la generación de informes en vivo y de historiales.

F. En la interfaz de usuario de la aplicación cliente, una tarea del tablero de control correspondiente al Monitoreo del Estado de Salud para proporcionar información en vivo, como gráficos circulares y listas de eventos, con el objetivo de evaluar de forma rápida y visual la salud general del sistema.

G. Un tablero de control del estado de salud centralizado basado en la web deberá estar disponible para visualizar las unidades y eventos de funciones del estado de salud de la USP de manera remota.

H. Estadísticas detalladas del cuidado del sistema estarán disponibles a través de un tablero de control basado en la web, y proporcionará métricas del estado de salud de las entidades y funciones de la USP, incluyendo tiempo activo y tiempo promedio entre fallas.

I. Todos los eventos generados en el sistema se pueden usar para automatizar la administración de eventos y acciones de la USP.

J. Los eventos del estado de salud serán accesibles a través del SDK (puede usarse para crear capturas de SNMP).

2.14 Requisitos Generales de la USP

A. La Plataforma Unificada de Seguridad (USP) deberá ser una solución de software clase empresarial de seguridad y protección habilitada para IP.

B. La USP deberá soportar la unificación transparente del Sistema de Control de Acceso IP (ACS), el Sistema de Administración de Videos IP (VMS), y el Sistema de Reconocimiento Automático de Placas de Matrícula IP (ALPR) bajo una sola plataforma. Las aplicaciones de interfaz de usuario (UI) de la USP deberán presentar una interfaz unificada de seguridad para la administración, configuración, monitoreo y generación de informes de los sistemas embebidos ACS, VMS y ALPR, y dispositivos periféricos asociados.

C. Las funcionalidades disponibles con la USP deberán incluir:

1. La configuración de sistemas embebidos, como los sistemas ACS, ALPR y VMS.
2. El monitoreo de eventos en vivo.

3. El monitoreo de video en vivo y reproducción de video archivado.
4. Administración de alarmas.
5. La generación de informes que incluyan la creación de plantillas de informes personalizados e informes de incidentes.
6. La característica de Federation para el monitoreo global, la generación de informes y la administración de alarmas de múltiples sistemas ACS, VMS y/o ALPR remotos e independientes esparcidos a lo largo de múltiples instalaciones y zonas geográficas. *(Especificador, solo Enterprise, se requiere licencia adicional)*
7. La administración global de tarjetahabientes a lo largo de múltiples instalaciones y zonas geográficas, cada una con su propio sistema ACS independiente. *(Especificador, solo Enterprise, se requiere licencia adicional para cada sitio)*
8. Integración de Microsoft Active Directory para la sincronización de las cuentas de usuarios de la USP y cuentas de tarjetahabientes del ACS. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
9. Dispositivo de intrusión e integración de paneles (monitoreo en vivo, generación de informes y armado/desarmado). *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
10. Integración de los dispositivos de Intercomunicador SIP para comunicación bidireccional. *(Especificador, todas las versiones, se requiere licencia adicional)*
11. Integración con sistemas y bases de datos de terceros a través de plug-ins (control de acceso, analíticas de video, puntos de venta, y otros.). *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
12. Visualización de mapas gráficos dinámicos.
13. Integración del sistema de administración de activos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

D. La USP deberá ser instalada en uno o más de los siguientes tipos de instalaciones:

1. Acceso unificado, ALPR, plataforma de videos y cualquier combinación de los mismos.
2. Control de acceso independiente, ALPR o plataforma de video.
3. Acceso unificado y plataforma de video que federa con múltiples ACS, VMS y ALPR remotos.
4. Plataforma independiente de video que federa múltiples VMS remotos independientes.
5. Control de acceso independiente que federa múltiples ACS remotos independientes.
6. Control de acceso independiente que federa múltiples ALPR remotos independientes.

E. Concesión de licencias:

1. Se deberá aplicar una sola concesión de licencias central en el servidor de configuración.
2. No deberá existir un requisito de aplicar una licencia en todo servidor de computadora o estación de trabajo de cliente.
3. Con base en las opciones seleccionadas, se podrán habilitar o deshabilitar uno o más sistemas embebidos.

F. Requisitos de Hardware y Software:

1. Los sistemas de la USP y los embebidos (video, reconocimiento de placas de matrícula y control de acceso) deberán estar diseñados para ejecutarse sobre una plataforma estándar basada en PC equipada con el sistema operativo Windows. El sistema operativo preferido deberá ser coordinado con el Propietario siguiendo los sistemas operativos soportados por el fabricante.
2. El software básico del cliente/servidor será desarrollado en su totalidad usando la plataforma de software .NET de Microsoft y el lenguaje de programación C# (C-Sharp).
3. El(los) servidor(es) de base de datos de la USP deberá(n) estar desarrollado(s) sobre el Servidor SQL de Microsoft. La versión SQL preferida deberá coordinarse con el Propietario y ser compatible con la USP.
4. La USP deberá ser compatible con los ambientes virtuales, incluyendo VMware y Microsoft Hyper-V.
5. La USP deberá usar el desarrollo y las tecnologías de programación más recientes de interfaz de usuario (UI) como lo son Microsoft WPF (Windows Presentation Foundation), el lenguaje de marcado XAML, y la plataforma de software .NET.

2.15 Arquitectura de la USP

A. La USP estará basada en un modelo de cliente/servidor. La USP deberá consistir de un Módulo de Software de Servidor (SSM) estándar y Aplicaciones de Software del Cliente (CSA).

B. La USP deberá ser una solución habilitada para IP. Toda la comunicación entre el SSM y la CSA estará basada en el protocolo TCP/IP estándar y deberá usar la encriptación TLS con certificados digitales para proteger el canal de comunicación.

C. El SSM deberá ser un servicio Windows que se pueda configurar para que comience a funcionar cuando se inicia y ejecuta el sistema operativo en el fondo. El SSM deberá comenzar a funcionar automáticamente cuando se enciende la computadora sin importar si hay o no un usuario con sesión iniciada en la máquina.

D. Los usuarios podrán implementar el SSM en un solo servidor o a lo largo de varios servidores para una arquitectura distribuida. La USP no tendrá restricciones en cuanto al número de SSM instalados.

E. La USP deberá soportar el concepto de la Característica de Federation en donde se pueden enlazar múltiples instalaciones independientes ACS, VMS y ALPR en un solo sistema virtual grande para el monitoreo, generación de informes y gestión de alarmas centralizados. *(Especificador, solo Enterprise, se requiere licencia adicional)*

F. La USP deberá proteger contra la posible falla del servidor de la base de datos y continuar funcionando con soluciones estándar disponibles en el mercado .

G. La USP deberá soportar hasta mil instancias de CSA conectadas al mismo tiempo. Sin embargo, se puede instalar un número ilimitado de CSA en cualquier momento. *(Especificador, máximo 5 con Standard; máximo 10 con Professional; ilimitado con Enterprise)*

H. La USP deberá soportar un número ilimitado de registros e historial de transacciones (eventos y alarmas) con el máximo permitido limitado por la cantidad de disco duro disponible.

I. La USP deberá soportar la transmisión de video sin interrupción. La CSA deberá mantener las conexiones de video existentes activas en caso de que un SSM (con excepción del Archiver) no esté disponible.

J. Arquitectura con Base en Funciones:

1. La USP deberá consistir de una arquitectura con base en funciones, donde cada SSM hospeda una o más funciones.
2. Cada función deberá ejecutar un conjunto específico de tareas relacionadas al sistema principal, el reconocimiento automático de placas de matrícula automotriz (ALPR), videos (VMS) o funcionalidades de control de acceso (ACS), entre muchas otras más. La instalación deberá estar simplificada a través de la habilidad de la USP para permitir a los administradores:
    a. Instalar uno o varios SSM a lo largo de la red antes de activar las funciones.
    b. Activar y desactivar funciones según sea necesario en todos y cada uno de los SSM.
    c. Centralizar la configuración y administración de la función.
    d. Soporte de configuración remota.
    e. Mover las funciones desde un SSM a otro.
3. Cada función, cuando sea necesario, deberá tener su propia base de datos para almacenar eventos e información de configuración específica a la función.
4. Las funciones sin base de datos, como la característica de Federation, Active Directory, y Administración Global de Tarjetahabientes, deberán soportar el modo de espera muy próximo al tiempo real sin que se requiera software de conmutación por error de terceros.
5. Función del Directory:

a. La Función de Directory deberá administrar la base de datos central que contiene toda la información del sistema y la configuración de componentes de la USP.

b. La Función de Directory deberá autenticar usuarios y dar acceso a la USP con base en derechos o privilegios de acceso predefinidos del usuario y configuraciones de particiones de seguridad.

c. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes comunes a los subsistemas del ACS, ALPR y el VMS:

   i. Particiones de seguridad, usuarios y grupos de usuarios

   ii. Áreas

   iii. Zonas, reglas de enlace de entrada/salida (E/S) y comportamiento de salida personalizado

   iv. Alarmas. Horarios y tareas programadas

   v. Eventos personalizados

   vi. Macros o guiones personalizados

d. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al VMS:

   i. Servidores de video y sus periféricos (como audio, E/S y puertos serie)

   ii. PTZ.

   iii. Secuencias de cámaras

   iv. Horarios de grabación y archivamiento

e. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al ACS:

   i. Controladores de puertas, y módulos de entrada y salida (E/S)

   ii. Puertas, Elevadores y Reglas de acceso

   iii. Tarjetahabientes y grupos de tarjetahabientes, credenciales y plantillas para distintivos

f. La Función de Directory deberá soportar la configuración/administración de los siguientes componentes específicos al ALPR:

   i. Unidades y cámaras ALPR

   ii. Listas activas, listas de permisos y reglas de sobretiempo

6. La Función del Video Archiver será responsable de administrar las cámaras y los codificadores que controle y archive.

7. La Función del Media Router será responsable de enrutar los flujos de video y audio en redes locales y de área extensa, desde la fuente (como el DVS) hacia el destino (como la CSA).

8. La Función del Administrador de Acceso será responsable de la sincronización de las unidades de hardware de control de acceso bajo su control, como lo son los controladores de puerta y los módulos de E/S. Además esta función debe ser responsable de validar y registrar todas las actividades y eventos de acceso cuando los controladores de puertas y los módulos E/S están en línea.
9. La Función del Reconocimiento Automático de Placas de Matrícula (ALPR) será responsable de sincronizar las unidades fijas ALPR (cámaras) y aplicaciones ALPR móviles bajo su control. La Función de ALPR será responsable de registrar todas las actividades y eventos del ALPR.
10. La Función de Zone Manager será responsable de administrar todas las zonas de software (recopilación de entradas) y el registro de eventos de zona asociados. Las zonas deberán consistir de entradas de control de acceso y de dispositivos de video.
11. La Función de Monitoreo del Estado de Salud será responsable por el monitoreo y registro de eventos y advertencias del estado de salud desde varias aplicaciones de cliente, funciones, y servicios que forman parte de la USP. Esta función también será responsable de registrar eventos dentro del Windows Event Log y por generar informes sobre las estadísticas y el historial de salud.
12. Funciones Opcionales
    a. La Característica de Federation™ será responsable de crear un gran sistema virtual que consista de cientos o miles de sistemas ACS, VMS y/o ALPR independientes y remotos. *(Especificador, solo Enterprise, se requiere licencia adicional)*
    b. La Función del Global Cardholder Synchronizer será responsable de sincronizar la información de los tarjetahabiente y credenciales entre el sitio local y el sitio central. También deberá soportar la sincronización entre sitios remotos. *(Especificador, solo Enterprise, se requiere licencia adicional)*
    c. La Función del Active Directory será responsable de sincronizar las cuentas de los usuarios y cuentas de los tarjetahabientes con un servidor Microsoft Active Directory. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
    d. La Función del Intrusion Manager será responsable de administrar los dispositivos de intrusión de terceros como los paneles de alarmas y dispositivos de detección de perímetros. Esta función también será responsable de registrar de todos los eventos de intrusión en una base de datos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*
    e. La Función del Asset Manager será responsable de integrar y sincronizar los sistemas de administración de activos de terceros y eventos relacionados con el registro de activos. La función será responsable de soportar la ejecución de informes relacionados con activos como informes de inventarios e informes de actividad de activos. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

f. El Rol de Plugin Manager será responsable por la comunicación entre la USP y los sistemas de terceras partes como lo son datos analíticos de video, ALPR, controles de acceso, video y sistemas de gestión de edificios. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

g. La Función del Point of Sale (POS, por sus siglas en inglés) será responsable de integrar la USP con sistemas POS de terceros y de registrar las transacciones. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

h. La Función de Web SDK será responsable de conectar la USP a cualquier aplicación o interfaz desarrollada con el Web Service SDK. Las aplicaciones desarrolladas con el Web Service SDK serán independientes de la plataforma y dependerán del protocolo REST para las comunicaciones. *(Especificador: se requiere licencia adicional para Professional y versiones superiores)*

i. La Función Communication Management será responsable de registrar los extremos de comunicación SIP y por administrar el enrutamiento de las llamadas. *(Especificador, todos los paquetes, se requiere licencia adicional)*

j. La Función de Video Redirector será responsable de conectar cualquier transmisión de video a un sistema de terceros que use el protocolo estándar RTSP. Esta función deberá proporcionar acceso a video en vivo. *(Especificador, Professional y versiones superiores, se requieren paquetes de SDK, se requiere licencia adicional)*

K. Servicio de Monitoreo de Servidores (Watchdog):

1. La USP deberá incluir un Servicio de Monitoreo de Servidores que monitoree continuamente el estado del servicio del Módulo de Software del Servidor (SSM).

2. El Servicio de Monitoreo de Servidores será un servicio Windows que se inicia de forma automática en el encender el sistema, sin importar si el usuario está conectado o no a su cuenta.

3. El Servicio de Monitoreo de Servidores estará instalado en todos los servidores y PC que ejecutan un SSM. En caso de fallas o funcionamiento defectuoso, el Servicio de Monitoreo de Servidores deberá reiniciar el servicio averiado. Como último recurso, el Servicio de Monitoreo de Servidores deberá reiniciar el servidor/PC si no fuera posible reiniciar el servicio.

2.16 Control de acceso USP, video y unificación ALPR

A. El Monitoreo UI deberá presentar una verdadera Interfaz de Seguridad Unificada para el monitoreo y los informes en vivo del ACS, el VMS y el ALPR. La visualización y reproducción avanzada de vídeo en vivo de vídeo archivado deberá estar disponible a través de la UI de Monitoreo.

B. La configuración de UI deberá presentar una verdadera Interfaz de Seguridad Unificada para la configuración y administración del ACS, el VMS y el ALPR.

C. El usuario deberá ser capaz de asociar una o más cámaras de video a los siguientes tipos de entidad: áreas, puertas, elevadores, zonas, alarmas, paneles de intrusión, cámaras ALPR y más.

D. Será posible ver el video asociado con los eventos de control de acceso cuando se visualiza un informe.

E. Será posible ver el video asociado con los eventos de los paneles de intrusión cuando se visualiza un informe.

F. Deberá ser posible ver el video asociado con los eventos del ALPR cuando se visualice un informe.

G. La USP deberá soportar la siguiente funcionalidad de la Administración de Alarmas:

1. Crear y modificar alarmas definidas por el usuario. Deberá soportar un número ilimitado de alarmas definidas por el usuario.
2. Asignar un cronograma de tiempo o período de cobertura a una alarma. Deberá activarse una alarma solamente si es una alarma válida para el período de tiempo actual.
3. Establecer el nivel de prioridad de una alarma y su umbral de reactivación.
4. Definir si se visualiza video en vivo o grabado, imágenes fijas o una mezcla de estos una vez que se activa una alarma.
5. Proporcionar la habilidad de visualizar video en vivo y grabado dentro del mismo recuadro de video utilizando el modo imagen en imagen (PiP).
6. Proporcionar la habilidad de agrupar alarmas por fuente y por tipo.
7. Definir un período de tiempo después del cual se reconoce de forma automática la alarma.
8. Definir los destinatarios de una alarma. Las notificaciones de alarmas deberán distribuirse a uno o más destinatarios. Los destinatarios deberán recibir un nivel de prioridad que jerarquice el orden de recepción de una alarma.
9. Definir el modo de transmisión de la alarma. Las notificaciones de alarmas se enviarán usando un modo de transmisión secuencial o un modo de transmisión de todo a la vez.
10. Definir si se visualiza la fuente de la alarma, una o más entidades o una página HTML.
11. Especificar si es obligatorio la generación de un informe de incidente durante el reconocimiento.

H. Los flujos de trabajo para crear, modificar, agregar instrucciones y procedimientos, y reconocer una alarma deberán ser consistentes para las alarmas de control de acceso, ALPR y videos.

I. Las alarmas deberán ser federadas, permitiendo la gestión global de alarmas a lo largo de múltiples sistemas independientes USP, ACS, VMS y ALPR.

J. La USP deberá además soportar la notificación de alarmas a una dirección de correo electrónico o a cualquier dispositivo que usa el protocolo SMTP.

K. La habilidad para crear instrucciones relacionadas con las alarmas será soportada a través de la visualización de una o más páginas HTML después de un evento de alarma. Las páginas HTML deberán ser definidas por el usuario y se podrán vincular entre sí.

L. Deberá soportarse el empaque y desempaque de la alarma en donde todas las entidades relacionadas con una alarma se puedan visualizar en la UI de Monitoreo con un simple clic de un botón.

M. El usuario tendrá la habilidad de reconocer alarmas, crear un incidente al reconocer una alarma, y colocar una alarma en el modo repetición.

N. El usuario deberá ser capaz de activar alarmas de forma espontánea con base a lo que vea en el sistema.

O. Una alarma deberá estar configurada de tal forma que permanezca visible hasta que se reconozca la condición de la fuente.

P. El usuario será capaz de investigar la alarma sin tener que reconocerla.

2.17 Niveles de amenaza de la USP *(Especificador: se requiere licencia adicional; solo Enterprise)*

A. La USP deberá soportar los Niveles de Amenaza para cambiar de forma dinámica el comportamiento del sistema para responder a eventos críticos.

B. Los Niveles de Amenaza deberán activarse y desactivarse por el operador de la CSA con el privilegio adecuado.

C. Los Niveles de Amenaza deberán establecerse en un área o en todo el sistema.

D. Los Niveles de Amenaza afectarán el comportamiento del sistema al ejecutar cualquier acción disponible en la USP, como: activar salida, iniciar la grabación, bloquear cámaras, invalidar la calidad de la grabación, armar una zona, colocar una puerta en un modo de mantenimiento, y otros.

E. Deberán estar disponibles las siguientes acciones específicas con los Niveles de Amenaza:

1. Establecer una autorización de seguridad mínima para restringir o permitir el acceso de tarjetahabientes a áreas específicas además de otras restricciones impuestas por las reglas de acceso.

2. Establecer un nivel de usuario mínimo para cerrar automáticamente la sesión del usuario en la USP.

3. Establecer el modo de lector para cambiar la forma de obtener acceso a las puertas (por ejemplo, tarjeta y PIN, o tarjeta o PIN).

F. Se deberá visualizar una notificación visible en toda la CSA del operador cuando se active un Nivel de Amenaza.

2.18 Tarea de la USP remota

A. La USP deberá proporcionar, mediante una Tarea Remota, capacidades para monitorear y controlar de forma remota el contenido de otras estaciones de trabajo que están ejecutando la CSA (UI de Monitoreo) que forman parte del mismo sistema.

B. La USP deberá soportar aplicaciones para paredes de video al conectar y controlar múltiples estaciones de trabajo y monitores de forma simultánea.

C. La Tarea Remota será una interfaz gráfica que muestra la replicación de la estaciones de trabajo remota que están ejecutando la CSA (UI de Monitoreo).

D. La Tarea Remota deberá permitir la conexión a otras estaciones de trabajo que usan un modo de ancho de banda bajo para recibir instantáneas de datos de video visualizado de forma remota.

E. La Tarea Remota deberá permitir la conexión a otras estaciones de trabajo que usan un modo de espía para permanecer invisibles a la estación de trabajo conectada de forma remota. La opción de modo espía deberá estar disponible para los usuarios con permisos para tener acceso a dicha función.

F. La funcionalidad ofrecida por la capacidad de monitoreo y control remoto deberá incluir:

1. Monitoreo remoto y control del monitoreo y las tareas de monitoreo de alarmas.
2. Habilidad para intercambiar cámaras, puertas y zonas de forma remota en los recuadros de visualización.
3. Habilidad para controlar el video en vivo y en reproducción de forma remota.
4. Habilidad para cambiar el patrón del recuadro de forma remota.
5. Habilitad para crear y eliminar tareas de forma remota.
6. Habilidad para iniciar/detener de forma remota los ciclos de las tareas.
7. Habilidad para ir al modo de pantalla completa de forma remota.
8. Habilidad para guardar y volver a cargar el área de trabajo de forma remota.

2.19 Administración Avanzada de Tareas de la USP

A. La USP deberá soportar una infraestructura para administrar las tareas de la UI de Monitoreo que se usan para el monitoreo en vivo, las actividades diarias y la generación de informes.

B. Los administradores deberán ser capaces de asignar tareas y bloquear el área de trabajo del operador. La administración del usuario de su área de trabajo deberá estar limitada por sus privilegios asignados.

C. Los operadores deberán ser capaces de guardar sus tareas ya sea como Tareas Públicas o Tareas Privadas, y en una partición específica. Las Tareas Públicas

deberán estar disponibles para todos los usuarios. Las Tareas Privadas solo deberán estar disponibles para el propietario de la tarea.

D. Los operadores deberán ser capaces de compartir sus tareas enviándolas a uno o más usuarios en línea. Los destinatarios deberán tener la opción de aceptar la tarea enviada.

E. Los operadores deberán ser capaces de duplicar una tarea.

2.20 Informes de la USP

A. La USP deberá soportar la generación de informes (informes de base de datos) para el control de acceso, ALPR, videos e intrusión.

B. Todos y cada uno de los informes en el sistema deberá ser una tarea de la USP, cada una asociada con su propio privilegio. Un usuario deberá tener acceso a una determinada tarea de informe si cuenta con los privilegios correspondientes.

C. Los flujos de trabajo para crear, modificar, y ejecutar un informe deberán ser consistentes para los informes de control de acceso, ALPR y video.

D. Los informes deberán ser federados, lo que permite la generación de informes globales consolidados a lo largo de múltiples sistemas independientes USP, ACS, VMS y ALPR.

E. Los informes de control de acceso y ALPR deberán soportar las fotos de los tarjetahabientes y fotos de las placas de matrícula, respectivamente.

F. La USP deberá soportar los siguientes tipos de informes:

1. Informes de alarmas
2. Informes específicos de video (archivos, marcadores, movimiento y otros)
3. Informes de configuración (tarjetahabientes, credenciales, unidades, reglas de acceso, lectores/entradas/salidas y más)
4. Informes de actividades (tarjetahabientes, grupo de tarjetahabientes, visitantes, credenciales, puertas, unidades, áreas, zonas, elevadores y más)
5. Informes específicos de ALPR (reproducción de ALPR móvil, aciertos, lecturas de placas, lecturas/aciertos por día, lecturas/aciertos por zona de ALPR y demás)
6. Informes de actividad del estado de salud y estadísticas del estado de salud
7. Otros tipos de informes, como informes de visitantes, informes de registros de auditoría, informes de incidentes e informes de horario y asistencia

G. Informes Genéricos, Informes Personalizados y Plantillas de Informes

1. El usuario deberá tener la opción de generar informes genéricos desde una lista existente, generar informes desde una lista de plantillas definidas por el usuario, o crear un nuevo informe o una plantilla de informe.

2. El usuario deberé ser capaz de personalizar informes predefinidos y guardarlos como nuevas plantillas de informe. No existirá la necesidad de una herramienta externa de generación de informes para crear informes personalizados y plantillas de informe. Las opciones de personalización incluirán la configuración de filtros, extensión del informe, y período de tiempo de espera. El usuario también deberá ser capaz de establecer cuales columnas serán visibles en un informe. La clasificación de los datos reportados estará disponible haciendo clic en la columna correspondiente y seleccionando un criterio de clasificación (ascendente o descendente).
3. Todas las plantillas de informes deberán crearse dentro de la UI de Monitoreo.
4. Estas plantillas se pueden usar para generar informes sobre un cronograma en formato PDF o Excel.
5. Un número ilimitado de informes y plantillas personalizadas serán soportados.

H. El diagrama de una tarea de generación de informes deberá consistir de paneles con configuraciones (duración de informe, filtros, mandos 'ir a' y 'restablecer', etc.), los datos actuales del informe en formato de columna, y un panel con recuadros de visualización. El usuario deberá ser capaz de arrastrar y soltar registros individuales en un informe sobre uno o más recuadros de visualización para ver la foto de identificación de un tarjetahabiente, reproducir una secuencia de video, o un evento ALPR.

I. La USP deberá soportar el filtrado completo de datos para la mayoría de los informes con base en el tipo de entidad, tipo de evento, marca de tiempo del evento, campos personalizados, etc.

J. La tarea de informe tendrá la capacidad de mostrar resultados a través de gráficos, como gráficos de líneas, gráficos de barras, gráficos de barras apiladas, gráficos de anillos y gráficos circulares.

K. El usuario deberá ser capaz de hacer clic sobre una entidad dentro de un informe existente para generar informes adicionales desde la UI de Monitoreo.

L. La USP deberá soportar las siguientes acciones en un informe: imprimir el informe, exportar el informe a un archivo PDF/Microsoft Excel/CSV, exportar los gráficos en formato JPG/PNG y enviar de manera automática por correo electrónico un informe en función de un horario y una lista de uno o más destinatarios.

2.21 Tableros de la USP

A. La USP deberá ser capaz de crear tableros.

B. Los operadores deberán poder ver los tableros si cuentan con los privilegios correspondientes. Los usuarios con los privilegios correspondientes también deberán ser capaces de modificar los tableros.

C. Los tableros del sistema deberán ser una tarea de la USP. Un usuario deberá tener acceso a una tarea específica de tablero si cuenta con los privilegios correspondientes.

D. Los tableros se deberán guardar en una carpeta privada o pública.

E. Un tablero deberá estar formado por un área de trabajo con varios widgets que aparezcan en dicha área. Todos los widgets deberán proporcionar la capacidad de especificar su ubicación y tamaño, un título y un color de fondo, y de ofrecer la capacidad de actualizar su contenido con frecuencia.

F. Tipos de widgets para tableros:

1. Imagen: ofrece la capacidad de mostrar una imagen (JPG, PNG, GIF y BMP) en un tablero.
2. Texto: ofrece la capacidad de mostrar texto en un tablero. El estilo del texto deberá poder configurarse, de manera que el usuario pueda especificar la fuente, el tamaño, el color y la alineación.
3. Mosaico: ofrece la capacidad de mostrar cualquier entidad de la USP en un mosaico.
4. Página web: ofrece la capacidad de mostrar una URL en un tablero.
5. Cantidad de entidades: ofrece la capacidad de mostrar la cantidad total de un determinado tipo de entidad en la USP.
6. Informes: ofrece la capacidad de mostrar los resultados de los informes guardados en el sistema. Los resultados se visualizarán mostrando la cantidad total de resultados en el informe, un conjunto de los principales resultados del informe o un gráfico visual de los datos del informe.

G. Será posible ampliar los widgets de un tablero con un SDK. De esta forma, se podrán desarrollar widgets personalizados para el sistema.

H. La USP deberá soportar las siguientes acciones en un tablero: imprimir el tablero, exportar el tablero a un archivo PNG y enviar automáticamente por correo electrónico un informe en función de un horario y una lista de uno o más destinatarios.

2.22 Característica de Federation de la USP: Monitoreo de sistemas remotos *(Especificador: solo Enterprise, licencia adicional obligatoria para cada sitio y entidad federada.)*

A. La USP deberá soportar el concepto de una función federada para el control de acceso, video y ALPR.

B. La característica de Federation permitirá la unificación de múltiples sistemas USP independientes (sistemas Federados) en un solo sistema virtual más grande (la característica de Federation). Esto deberá facilitar el monitoreo global de múltiples sistemas USP independientes.

C. La característica de Federation deberá soportar la unificación de múltiples sistemas independientes de videovigilancia o VMS.

D. Las entidades que se federarán y monitorearán de forma centralizada desde la característica de Federation deberán incluir alarmas, áreas, cámaras, tarjetahabientes y grupos de configuración de tarjetahabientes, credenciales, puertas, elevadores, eventos ALPR y zonas (entradas monitoreadas).

E. La característica de Federation deberá soportar una integración basada en nube, por medio de la cual se actualizarán de forma automática el servicio e infraestructura y la proporcionará el proveedor del servicio, sin la necesidad de hardware en el sitio.

F. La característica de Federación deberá soportar la Gestión Global de Alarmas, desde el monitoreo de UI para el control de acceso, video y ALPR.

G. La función de federación deberá soportar la Generación Global de Informes desde el monitoreo de UI para el control de acceso, video y ALPR.

H. La característica de Federation deberá soportar docenas de acciones del operador en entidades remotas (federadas) desde la UI de Monitoreo (por ejemplo, generar un informe global tomando en cuenta eventos de múltiples sitios independientes o reconocer alarmas remotas).

2.23 Administración de Zonas de la USP

A. La USP deberá soportar la configuración y administración de las zonas para el monitoreo del punto de entrada a través de la Función del Zone Manager. Un usuario podrá agregar, borrar o modificar una zona si cuenta con los privilegios correspondientes.

B. Una zona deberá monitorear el estado de uno o más puntos de entrada. Deberá ser posible el monitoreo de la zona o de un punto de entrada a través del uso de un controlador y uno o más módulos de entrada. Las entradas desde las cámaras o codificadores de video también deberán estar accesibles a través de una zona.

C. Dependiendo del hardware que está instalado deberán soportarse las entradas supervisadas. Dependiendo del módulo de entrada usado se deberá tener disponibilidad de supervisión tanto de 3 como de 4 estados.

D. Se deberá definir un cronograma para una zona indicando cuándo se monitoreará la zona.

E. Los Eventos Personalizados deberán ofrecer una flexibilidad completa para crear eventos personalizados específicos a una zona. El usuario será capaz de asociar los eventos personalizados a los cambios de estado en las entradas monitoreadas.

F. El ACS deberá soportar una o más cámaras por zona. Videos deberán estar asociados a los cambios de estado de una zona.

G. Enlace de Entrada/Salida (E/S):

1. La administración de las zonas deberá soportar la Vinculación de Entrada/Salida (E/S). El enlace de E/S deberá permitir que una o más entradas activen una o más salidas.

2. El enlace de E/S deberá estar disponible en el modo fuera de línea cuando la comunicación entre el servidor y el hardware no está disponible.

3. Los Comportamientos de Salida Personalizados deberán ofrecer completa flexibilidad para crear una variedad de patrones complejos de señal de salida: pulsos simples, pulsos periódicos, pulsos de ciclo variable, y cambios de estado.

4. A través de la acción de 'activación de salida', el ACS deberá soportar la activación de salidas con comportamientos de salida personalizados.

2.24 Administración de Seguridad del Usuario y Grupo de Usuarios, Particiones y Privilegios de la USP

A. La USP deberá soportar la configuración y la administración de usuarios y grupos de usuarios. Un usuario podrá agregar, borrar o modificar un usuario o grupo de usuarios si cuenta con los privilegios correspondientes.

B. La USP deberá soportar la autenticación de usuario con autenticación basada en notificaciones usando proveedores externos. Los proveedores externos deberán incluir:

1. ADFS (Servicios de federación de Active Directory)
2. Azure Active Directory (a través de OpenID Connect)
3. Ping Identity (a través de OpenID Connect)
4. KeyCloak (a través de OpenID Connect)
5. Otros agentes de autenticación de Open ID Connect/SAML2

C. Los derechos y privilegios de acceso comunes compartidos por múltiples usuarios deberán definirse como Grupos de Usuarios. Los miembros individuales del grupo deberán heredar los derechos y privilegios de sus grupos de usuarios primario. Se permitirá el anidamiento de grupo de usuarios.

D. Los privilegios del usuario deberán ser amplios en la USP. Todas las entidades configurables para la USP, incluyendo el control de acceso, video y ALPR, deberán contar con privilegios asociados.

E. Las entidades específicas, como tarjetahabientes, grupos de tarjetahabientes, y credenciales, deberán incluir un juego de privilegios más pormenorizado, como el derecho al acceso a campos personalizados y cambio de activación o estado del perfil de una entidad.

F. Particiones:

1. La USP deberá limitar lo que pueden ver los usuarios en la base de datos de configuración a través de particiones de seguridad (segmentos de base de datos). El administrador, quien cuenta con todos los derechos y privilegios, tendrá permitido segmentar un sistema en múltiples particiones de seguridad.
2. Todas las entidades que forman parte de la USP se pueden asignar a una o más particiones.
3. Un usuario que reciba acceso a una partición específica solo deberá ser capaz de ver las entidades (componentes) dentro de la partición a la cuál ha sido asignado. El acceso se otorga al asignar al usuario como un usuario aceptado para ver las entidades que forman parte de una partición en particular.
4. Un usuario o grupo de usuarios puede recibir derechos de administrador sobre la partición.

G. Deberá ser posible especificar el usuario y los privilegios del grupo de usuarios con base en la partición.

H. Las opciones avanzadas de inicio de sesión deberán estar disponibles como inicio de sesión doble, y otros.

I. Deberá ser posible especificar un período inactivo para la UI de Monitoreo y después de dicho tiempo la aplicación se bloqueará de forma automática, al mismo tiempo que conserva el acceso a las señales de la cámara visualizadas actualmente.

J. Será posible revisar los permisos de los usuarios y determinar lo siguiente:

1. El usuario o grupo de usuarios que pueden ver o modificar una entidad del sistema.
2. Los privilegios de cada usuario o grupo de usuarios del sistema.
3. El usuario o grupo de usuarios que puede realizar la acción vinculada a un privilegio

2.25 Administración de evento/acción de la USP

A. La USP deberá soportar la configuración y la administración de eventos para videos y ALPR. Un usuario será capaz de agregar, eliminar o modificar una acción enlazada a un evento si cuenta con los privilegios correspondientes.

B. El USP recibirá todos los eventos entrantes de uno o más ACS, VMS y ALPR. La USP deberá tomar las acciones correspondientes con base a relaciones de eventos/acciones definidas por el usuario.

C. La USP deberá recibir y registrar los siguientes eventos:

1. Eventos en todo el sistema
2. Eventos de aplicación (clientes y servidores)
3. Eventos de áreas, cámaras, puertas, elevadores y ALPR (lecturas y aciertos)
4. Eventos de unidad
5. Eventos de zona
6. Eventos de alarmas
7. Eventos ALPR
8. Eventos de Monitoreo del Estado de Salud

D. La USP deberé permitir la creación de eventos personalizados.

E. La USP deberá contar con la capacidad para ejecutar una acción en respuesta a un evento de control de acceso, video y ALPR. La USP deberá soportar la siguiente lista de acciones, sin estar limitada a:

1. Agregar marcadores

2. Bloquear y desbloquear video
3. Visualizar una cámara en un monitor analógico
4. Visualizar una entidad en la CSA
5. Mandar un informe por correo electrónico
6. Mandar una instantánea por correo electrónico
7. Exportar un informe
8. Ir a la página de inicio
9. Ir a preestablecidos
10. Invalidar la calidad de grabación
11. Reproducir un sonido
12. Reiniciar una unidad
13. Ejecutar una macro
14. Ejecutar un patrón
15. Enviar un mensaje
16. Enviar un correo electrónico
17. Establecer un nivel de amenaza
18. Iniciar/detener la aplicación de protección de video
19. Iniciar / detener grabación
20. Iniciar / detener transferencia
21. Activar alarma
22. Desencadenar una salida

F. La USP deberá permitir que un horario se asocie con una acción. Deberá activarse la acción solamente si es una acción adecuada para el período de tiempo actual.

2.26 Programas y tareas programadas de la USP

A. Programaciones

1. La USP deberá soportar la configuración y la administración de cronogramas complejos. Un usuario podrá agregar, borrar o modificar un horario si cuenta con los privilegios correspondientes.
2. La USP deberá ofrecer total flexibilidad y la capacidad de detallar cuando se crea un cronograma. El usuario deberá ser capaz de definir un cronograma en incrementos de 1 o 15 minutos.
3. Deberán soportarse programas diarios, mensuales, ordinales y específicos.

B. Tareas Programadas

1. La USP deberá soportar tareas programadas para video y ALPR.
2. Las tareas programadas deberán ejecutarse en un horario definido por el usuario en un día y hora específico. También deberá soportar tareas periódicas o recurrentes bajo un cronograma.
3. Las tareas programadas deberán soportar todas las acciones estándar disponibles dentro de la USP, como enviar un correo electrónico o enviar un informe por correo electrónico.

2.27 Macros y Scripts Personalizados de la USP

A. La USP deberá habilitar a los usuarios a automatizar y ampliar las funcionalidades del sistema a través del uso de macros o scripts personalizados para el control de acceso, video y ALPR.

B. Los macros personalizados deberán crearse con el Kit de Desarrollo de Software (SDK) de la USP.

C. Una macro deberé ejecutarse tanto de forma automática como manual.

D. Se deberá lanzar una macro en la UI de Monitoreo a través de acciones activas.

2.28 Mapas gráficos dinámicos (DGM) de la USP

A. La USP deberá soportar la funcionalidad de mapeo para el control de acceso, videovigilancia, detección de intrusión, ALPR y aplicaciones externas.

B. La USP deberá proporcionar una interfaz centrada en mapas con la habilidad de comando y control de todas las capacidades de la USP desde una interfaz de mapa de pantalla completa.

C. Deberá ser posible extender el mapa sobre todas las pantallas de la estación del cliente de la USP. En el escenario en donde el mapa se extiende sobre todas las pantallas de la estación del cliente de la USP, deberá ser posible navegar el mapa incluyendo panorámica y zoom, y los movimientos del mapa deberán estar sincronizados en todas las pantallas. La expansión del mapa en varias pantallas debe ofrecer las mismas capacidades de mando y control que la visualización en una sola pantalla.

D. Los DGM deberán soportar los siguientes formatos de archivos y protocolos para la importación de los fondos mapas:

1. PDF
2. JPG
3. PNG
4. Servicio de Mosaico de Mapas Web (WMTS, por sus siglas en inglés) y Servicio de Mapas Web (WMS, por sus siglas en inglés) definidos por el Open Geospatial Consortium (OGC)
5. BeNomad

6. AutoCAD (DWG y DXF)

E. El DGM deberá proporcionar los siguientes proveedores de mapas en línea para usar como fondo de mapa y proporcionar la habilidad de administrar su licencia de servicio, si se requiere una:

1. Google Map, aéreo, topografía (Con licencia)
2. Bing Map, aéreo, satélite, híbrido (Con licencia)
3. ESRI ArcGIS (con licencia)
4. Mapa aéreo OpenStreet (con licencia)
5. OVI híbrido

F. Deberá ser posible configurar un conjunto de mapas mixtos elaborados por GIS, proveedores en línea y archivos privados importados, y enlazarlos todos juntos.

G. Los DGM deberán proporcionar la habilidad de visualizar todas las entidades nativas de la USP, entre las que se incluyen:

1. Cámaras, corregir y PTZ
2. Puertas
3. Secuencias de cámaras
4. Áreas
5. Áreas de intrusión
6. Zonas de intrusión
7. Cámaras de reconocimiento de placas de matrícula
8. Entradas digitales
9. Salidas digitales
10. Intercomunicador
11. Alarmas
12. Macros
13. Patrollers de Patrullas Policiales

H. Los DGM deberán proporcionar la habilidad de dibujar y mostrar información sobre el mapa en la siguiente forma:

1. Formas vectoriales: líneas, rectángulos, polígonos y elipses
2. Fotos
3. Texto

I. Los DGM deberán proporcionar la habilidad de visualizar cualquier tipo de entidades de terceros integradas mediante un SDK. *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

J. Los DGM deberán proporcionar la habilidad de mostrar capas de información en el formato Keyhole Markup Language (KML).

K. Los DGM deberán proporcionar la habilidad al operador de administrar capas de entidades visualizadas sobre el mapa, y ser capaz de encenderlas y apagarlas y cambiar el orden de superposición.

L. El DGM proporcionará la capacidad para importar capas de datos de uno o más servidores ESRI ArcGIS.

M. La DGM proporcionará a los operadores la capacidad para gestionar capas que son importadas de ESRI ArcGIS. Los usuarios podrán habilitar y deshabilitar las capas, además de clasificarlas.

N. El DGM ofrecerá una copia de seguridad y restauración de datos de mapas integrados para el fondo del mapa y las capas de entidades.

O. El DGM proporcionará la capacidad de importar configuraciones desde un archivo externo como:

1. Capa de AutoCAD para objetos
2. CSV, archivo de Excel

P. Los DGM deberán ofrecer capacidades de conmutación por error.

Q. Los DGM deberán ampliarse a varias miles de entidades sobre un solo mapa y cientos de mapas.

R. Los DGM deberán proporcionar un medio para actualizar el fondo de un mapa sin afectar la configuración del objeto de mapa.

S. Los DGM deberán ofrecer un diseñador de mapas gráficos fácil de usar para configurar los mapas.

T. Los DGM deberán proporcionar una navegación fácil e intuitiva que incluya:

1. La habilidad para crear jerarquías de mapas para facilitar la navegación dentro y entre varios sitios y edificios.
2. La habilidad para definir favoritos para una recuperación de posición recurrente.
3. La posibilidad de crear vínculos entre mapas. Los enlaces de los mapas deberán permitir el vínculo desde un mapa a múltiples mapas que representan los pisos de un edificio. Mantener el nivel de zoom del mapa cuando se navegue por el piso de un edificio
4. Una experiencia común de usuario en relación a la navegación en el mapa para GIS y para mapas privados. *(Especificador, se requiere Plan Manager Advanced para GIS)*

U. Deberá ser posible monitorear el estado de entidades en el mapa. Deberá ser posible personalizar los íconos de cualquier entidad representada en el mapa.

V. Los DGM deberán ofrecer la habilidad de establecer de forma opcional una notificación de visualización gráfica de la detección de movimiento.

W. Los DGM deberán ofrecer una herramienta inteligente de selección para tener acceso al video. Al hacer clic en la ubicación que el usuario quiere ver, el DGM seleccionará de forma automática las cámaras que pueden ver esta ubicación y mover el PTZ hacia dicha ubicación. Esta herramienta inteligente de selección deberá tomar en consideración los obstáculos y no mostrar las cámaras que no pueden ver la ubicación debido a una pared.

X. Deberá ser posible seleccionar una ubicación dibujando una zona de interés en los DGM y visualizar todas las entidades que forman parte de dicha zona de interés a la vez.

Y. El usuario deberá ser capaz de seleccionar y visualizar el contenido de múltiples entidades de la USP sobre el mapa en las ventajas emergentes.

Z. El usuario deberá ser capaz de mover, redimensionar y fijar las ventanas emergentes de la entidad USP sobre el mapa.

AA. Deberá ser posible tener acceso a video en vivo y en modo de reproducción desde el mapa.

BB. Deberá ser posible monitorear desde los DGM todas las notificaciones de eventos de entidades. El usuario deberá ser capaz de encender y apagar las notificaciones por entidad.

CC. Los DGM deberán ofrecer la habilidad de operar completamente el monitoreo de alarmas. Deberá ser posible:

1. Centrar el mapa sobre entidades relacionadas con la alarma.
2. Visualizar la notificación de Alarmas sobre el mapa, y tener acceso al video relacionado desde el mapa.
3. Activar y recibir alarmas.
4. Actuar sobre la alarma desde los DGM, incluyendo reconocimientos, reenvíos e investigación.
5. Visualizar que una alarma ocurrió en un mapa vinculado subyacente.

DD. Los DGM deberán proporcionar las siguientes capacidades de búsqueda:

1. Buscar y centrar por nombre de entidad.
2. Desde la Visualización de una entidad en la USP, ubique la entidad en el mapa y ofrezca la posibilidad de seleccionar otra cercana.
3. Por dirección postal, ciudad, punto de referencia, punto de interés (con licencia de geocodificador de Google, ESRI u otro proveedor).

EE. Cualquier actualización del contenido del mapa por parte de un administrador se enviará de forma inmediata y dinámica a todos los usuarios de DGM.

FF. El DGM deberá soportar el uso de mapas GIS, mapas privados o una combinación de ambos para el fondo del mapa. *(Especificador, se requiere Plan Manager Advanced para GIS)*

GG. El DGM deberá ser compatible con cualquier mapa compatible con GIS con el OGC y con WMTS y WMS de soporte. Esto incluye, más no se limita a, mapas ESRI. El DGM deberá permitir la selección de las capas GIS adecuadas. *(Especificador, se requiere Plan Manager Advanced para GIS)*

HH. Los DGM deberán proporcionar un diseñador de mapas intuitivo para el posicionamiento de la entidad sobre el mapa usando la opción arrastrar y colocar. Cualquier configuración deberá ser gráfica.

II. Será posible editar y configurar múltiples objetos del mapa a la vez.

JJ. Todas las modificaciones en el diseño del mapa se conectarán a un registro de auditoría.

KK. Estarán disponibles varias acciones dentro de los mapas para que se ejecuten con un doble clic simple e intuitivo, con un clic en el botón derecho o la funcionalidad de arrastrar y soltar. Los ejemplos de acciones disponibles a través de los mapas deberán incluir el desbloqueo de puertas y el reconocimiento de una alarma.

LL. Mediante las siguientes funcionalidades, los DGM deberán permitir la administración de alarmas de la USP desde el mapa: *(Especificador, Plan Manager Standard y versiones superiores, se requiere licencia adicional)*

1. Ubicar sobre el mapa entidades relacionadas con la alarma.
2. Mostrar entidades de la alarma con un icono específico, color, nivel de transparencia y velocidad de intermitencia.
3. Listar, seleccionar y ubicar alarmas.
4. Centrado automático del mapa sobre la alarma con mayor prioridad.
5. Manejar la alarma desde el mapa, incluyendo reconocimientos, reenvíos e investigaciones
6. Todos los contenedores del mapa, como puntos activos o enlaces de mapas, deberán reflejar el estado de la alarma de las entidades contenidas.

MM. Deberá ser posible agregar funcionalidad avanzada a objetos del mapa usando el SDK. Cualquier funcionalidad disponible mediante el SDK de la USP estará disponible dentro de los mapas. *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

NN. Los DGM deberán ofrecer la herramienta de lazo para:

1. Mostrar entidades en un sitio a través de una sola acción.
2. Activar una acción en todas las entidades de un sitio con un solo clic.

3. Editar múltiples entidades de un solo sitio en forma simultánea.

OO. Los DGM deberán permitir la visualización de las entidades de la USP seleccionadas desde el mapa sobre un monitor remoto (pared de video). *(Especificador: se requiere licencia adicional para el Plan Manager Standard y versiones superiores)*

PP. El DGM deberá permitir realizar búsquedas en el mapa por nombre de la entidad.

QQ. Los DGM deberán permitir el uso de la información KML de mapas superpuestos tanto para mapas GIS como privados. Los objetos movibles deberán estar soportados mediante el uso de KML. *(Especificador, solo Plan Manager Advanced, se requiere licencia adicional)*

RR. El Contratista deberá proporcionar licencias para cada entidad que requiere ser mostrada en los mapas gráficos. *(Especificador, las licencias se venden en paquetes con base en la cantidad de entidades, especificar la licencia de un sitio o ilimitado después de 1,000 entidades)*

2.29 Auditoría y Registros de Actividades de Usuario de la USP (Registros)

A. La USP deberá soportar la generación de registros de auditoría. Los registros de auditoría deberán consistir de registros de adiciones, eliminaciones y modificaciones del operador/administrador,

B. Los registros de auditoría deberán generarse como informes. Deberán contar con la capacidad de rastrear cambios dentro de períodos de tiempo específicos. También deberá ser posible la consulta sobre usuarios específicos, cambios, entidades afectadas y períodos de tiempo.

C. Para los cambios de configuración de entidades, el informe de registros de auditoría deberá incluir información detallada sobre el valor antes y después de los cambios.

D. La USP deberá soportar la generación de registros de actividad del usuario. Los registros de actividad del usuario deberán consistir de registros de la actividad del operador en la USP como inicio de sesión, cámaras vistas, eventos ALPR, impresión de tarjetas de identificación, exportaciones de videos y otros.

E. El ACS deberá soportar las siguientes acciones sobre un informe de registros de auditoría y actividad: impresión y exportación de informes a un archivo PDF/Microsoft Excel/CSV.

2.30 Informes de Incidentes de la USP

A. Los informes de incidentes deberán permitir al operador de seguridad crear informes sobre incidentes que se presentaron durante un turno. Serán soportados los informes de incidentes relacionados con video y los incidentes relacionados con el control de acceso.

B. El operador será capaz de crear informes de incidentes independientes o informes de incidentes enlazados con las alarmas.

C. El operador deberá ser capaz de vincular secuencias múltiples de video a un incidente, tener acceso a los mismos, y cambiar la fecha u hora de las secuencias posteriormente.

D. Deberá ser posible crear una lista de categorías de Incidentes, etiquetar una categoría a un incidente, y filtrar la búsqueda con la categoría como parámetro.

E. Los informes de incidentes deberán permitir la creación de un formulario personalizado sobre el cual se incluya la información sobre un incidente.

F. Los informes de incidentes deberán permitir agregar entidades, eventos y alarmas para soportar las conclusiones del informe.

2.31 Ingestión de datos de USP

A. La USP deberá permitir la posibilidad de importar datos externos de fuentes externas para mejorar la unificación de las fuentes de datos dentro de la USP.

B. Cada fuente de datos se definirá mediante un conjunto de campos y tipos de campo que describen la fuente de datos. Los tipos de campo serán:

1. Cadena
2. Entero de 32 bits y 64 bits
3. Número de coma flotante
4. Booleano
5. Marca de tiempo
6. Binario (en un archivo o base 64)

C. La visualización de cada punto de datos de una fuente de datos será configurable para determinar qué campos de los datos deben mostrarse. La configuración de cada campo debe ser:

1. Qué campos se muestran u ocultan
2. En qué orden se muestran los campos
3. Una etiqueta para especificar el nombre del campo (en formato clave:valor)
4. Una opción para especificar cómo mostrar el campo (valor de texto, imagen, valor del portapapeles, hipervínculo a una página web, hipervínculo a una entidad en el sistema, archivo de sonido)

D. Debe haber un privilegio disponible para cada fuente de datos para permitir/denegar el acceso a usuarios específicos y grupos de usuarios de la USP.

E. Los datos ingeridos estarán disponibles en el sistema de informes de la USP.

F. Los datos ingeridos estarán disponibles para mostrarse en los Tableros de control de la USP.

2.32 Integración de terceros de USP

A. Integración de Microsoft Active Directory *(Especificador: se requiere licencia para Professional y versiones superiores)*

1. La USP deberá soportar una conexión directa a uno o varios servidores de Microsoft Active Directory mediante la(s) Función(es) del Active Directory. La integración del Active Directory deberá permitir la sincronización de información desde el servidor del Active Directory a la USP.
2. La integración del Active Directory deberá permitir la administración central de los usuarios, grupos de usuarios, tarjetahabientes y grupos de tarjetahabientes de la USP.
3. La USP deberá ser capaz de conectarse y sincronizar datos desde múltiples servidores de Active Directory (hasta 10).
4. La USP deberá soportar la sincronización de Grupos Universales del Active Directory al igual que la de grupos de seguridad que pertenecen a otros dominios dentro del mismo bosque.
5. La USP deberá soportar la encriptación del Microsoft Active Directory usando LDAP SSL.
6. Al estar habilitado, el Active Directory deberá administrar el inicio de sesión del usuario a las aplicaciones de la USP del cliente a través de las credenciales Windows del usuario. El inicio de sesión a la USP deberá utilizar características de la administración de contraseña y autenticación nativa del Active Directory.
7. Deberá ser posible sincronizar las siguientes entidades de la USP y su información desde el Active Directory con la USP:
    a. Usuarios (nombre de usuario, nombre y apellido, dirección de correo electrónico, etc.)
    b. Grupos de usuarios (nombre del grupo de usuarios, descripción, y dirección del correo electrónico del grupo).
    c. Atributos del Active Directory a los campos personalizados de la USP
8. Al estar habilitado, la adición, eliminación o suspensión de la cuenta Windows del usuario en el Active Directory deberá resultar en la creación, eliminación o deshabilitación de la cuenta de usuario equivalente en la USP.
9. Los métodos de sincronización admitidos para adiciones, modificaciones y eliminaciones de entidades sincronizadas deberán incluir en el primer inicio de sesión (solo usuarios), sincronización manual y sincronización programada.
10. La USP deberá soportar las conexiones de los usuarios a través de organizaciones independientes al conectarse a un proveedor de identidad externo mediante una autenticación basada en notificaciones, como ADFS (Active Directory Federation Services), Azure Active Directory, otros proveedores de OpenID Connect y SAML2.

B. Integración de Detección de Intrusión *(Especificador, Standard, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte el documento de Plugins Compatibles con Security Center)*

1. La USP se deberá integrar con los paneles de intrusión y dispositivos de terceros mediante un SDK de Intrusión. La Función del Intrusion Manager deberá manejar las comunicaciones con los paneles de intrusión. Las comunicaciones con los dispositivos de intrusión deberán ser sobre comunicaciones en serie y/o una red IP.
2. Deberá ser posible la integración con los paneles de intrusión fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.
3. La funcionalidad disponible mediante la integración de dispositivos de intrusión con la USP deberá incluir lo siguiente (en donde sea soportado por el panel de intrusión):
    a. Armar y desarmar dispositivos de intrusión (de forma manual, programada o después de un evento de la USP).
    b. Activación o accionamiento de salidas de dispositivos de intrusión.
    c. Visualización de eventos y alarmas de intrusión.
    d. Vigilancia del estado, incluyendo el estado de armado de los dispositivos de intrusión.
    e. Verificación por video de eventos y alarmas de intrusión con paneles de video.
    f. Creación de zonas USP utilizando entradas de dispositivos de intrusión.
4. Los paneles de intrusión actualmente soportados incluyen:
    a. Paneles Bosch de la serie G
    b. Bosch Map 5000
    c. Paneles DSC de la serie Power
    d. Paneles DMP de la serie XR
    e. Paneles Honeywell Galaxy Dimension y Flex
    f. Vanderbilt SPC
    g. UTC Advisor Master y Advanced
5. Los siguientes son algunos de los dispositivos de Intrusión adicionales compatibles:
    a. BuyTime
    b. Receptor de panel de alarmas
    c. Southwest Microwave RPMII

C. Sistemas de control de acceso de terceros *(Especificador: se requiere licencia adicional para Professional y versiones superiores; para obtener una lista extendida, consulte la guía de Plugins compatibles de Security Center)*

1. La USP deberá integrarse con software de control de acceso de terceros a través del SDK. Las comunicaciones con software de control de acceso se producirán a través de una red IP y no deberían soportar tareas administrativas como la administración de tarjetahabientes.
2. Deberá ser posible la integración con software de control de acceso fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.
3. La funcionalidad disponible mediante la integración de software de control de acceso con la USP deberá incluir lo siguiente (en donde sea soportado por la solución de control de acceso):
    a. Sincronice entidades de control de acceso y reciba estados y eventos asociados dentro de la USP, lo que incluye:
        i. Derechos de acceso y tarjetahabientes
        ii. Visitantes
        iii. Lectores y puertas
        iv. Alarmas
        v. Entradas y salidas
    b. Monitorear eventos de control de acceso.
    c. Monitorear y reconocer alarmas de control de acceso.
    d. Activar acciones y salidas en el software de control de acceso usando acciones activas y eventos a toma de acción.
    e. Bloquear y desbloquear puertas en el software de control de acceso.
    f. Verificación por video de eventos y alarmas de control de acceso.
    g. Configurar eventos a toma de acción usando los eventos y las alarmas de control de acceso.
    h. Generar informes de Security Center mediante el uso de datos de control de acceso.
    i. Visualizar y monitorear estados de entidades de puertas en los mapas de la USP.
4. Entre los fabricantes de control de acceso actualmente compatibles, se encuentran los siguientes:
    a. Tyco Softwarehouse CCURE
    b. UTC Lenel Onguard
    c. Amag Symmetry

d. Siemens Sipass

e. AssaAbloy ARX

D. Sistemas de Distribución de Destinos de Terceros: *(Especificador, Professional y versiones superiores, se requiere licencia adicional; para obtener una lista completa, consulte la guía de Plugins compatibles con Security Center)*

1. La USP deberá integrarse con software de distribución de destinos (control de elevadores) de terceros a través del SDK. Las comunicaciones con el software de distribución de destinos se deberán realizar en una red IP.
2. Deberá ser posible la integración con software de distribución de destinos fuera del ciclo de liberación de la USP. Deberá ser posible agregar nuevas integraciones en cualquier momento.
3. La funcionalidad disponible mediante la integración de software de distribución de destinos con la USP deberá incluir lo siguiente (en donde sea soportado por la solución de distribución de destinos):
   a. Creación de entidades de la distribución de destinos y recepción de eventos y estados relacionados dentro de la USP, incluyendo lo siguiente:
      i. Pisos y descansos
      ii. Carros de elevadores (puertas delanteras y traseras) y quioscos
      iii. Tarjetahabientes y credenciales (si corresponde)
   b. Monitoreo de eventos de distribución de destinos.
   c. Activación de acciones manuales de distribución.
   d. Verificación por video de eventos de distribución de destinos.
   e. Configuración de eventos a toma de acción mediante eventos de distribución de destinos.
   f. Generación de informes de Security Center con los datos de la distribución de destinos.
   g. Compatibilidad con varios lectores:
      i. Lectores internos de quioscos
      ii. Lectores de la USP
   h. Tipos de pasajeros y modos avanzados de quioscos.
4. Entre los fabricantes de distribución de destinos actualmente compatibles, se incluyen los siguientes:
   a. Otis Compass
   b. Thyssenkrupp
   c. Schindler
   d. MCE

E. Integración de gestión de activos *(Prescriptor, profesionales y superiores, requiere licencia adicional)*

1. La USP se deberá integrar con los sistemas de administración de activos de terceros mediante la Función de Administración de Activos.
2. Las comunicaciones con las soluciones de la administración de activos deberán ser sobre una red IP (mediante comunicaciones de software).
3. La funcionalidad disponible mediante la integración de sistemas de administración de activos con la USP deberá incluir lo siguiente (en donde lo soporten los sistemas de administración de activos):
    a. Sincronización de los activos del sistema de administración de activos con las entidades de activos de la USP.
    b. Monitoreo en vivo de los eventos de actividades relacionadas con activos, eventos de los estados de salud y actividad (activo en línea, activo fuera de línea, movimientos de activo o baja batería).
    c. Sincronización de alarmas de administración de activos con las alarmas del Security Center.
    d. Visualización de video enlazado a actividades y alertas relacionadas con activos dentro de las tareas de generación de informes y monitoreo.
    e. Reconocimiento de alarmas en Security Center el cual reconoce alertas en el sistema de administración de activos y viceversa.
    f. Seguimiento en tiempo real de ubicaciones de activos por áreas.
    g. Tarea de generación de informes de Inventario de Administración de Activos que muestra a detalle la ubicación actual (área) de un activo.
    h. Tarea de generación de informes de Actividad de Activos que proporciona un resumen histórico de eventos y actividades relacionadas con activos.
4. Los sistemas de administración de activos actualmente compatibles incluyen:
    a. Administración de claves Deister
    b. Morsewatchmans
    c. TRAKA

F. Integraciones Adicionales de Terceros

1. La USP deberá soportar enfoques múltiples para la integración de sistemas de terceros. Estas deberán incluir: Kits de Desarrollo de Software (SDK), SDK de Servicio de Web basado en REST, SDK de Servicio RTSP, entre otros. *(Especificador, Professional y versiones superiores, se requiere licencia y paquete SDK)*
2. La arquitectura de la USP deberá soportar la adición de nuevas conexiones para adaptarse a la integración de sistemas de terceros, por ejemplo: *(Especificador: consulte el sitio web para ver cómo se otorgan las licencias; para obtener una*

lista actualizada de las integraciones de terceros, consulte la guía de plugins compatibles)

a. Video analíticas
b. Sistemas de video de terceros
c. Sistemas de control de acceso de terceros
d. Integraciones de ALPR con estaciones de pago, proveedores de permisos, proveedores de pagos por teléfono y vendedores de boletos
e. Sistemas de administración de edificios
f. Ecosistema de Control de Acceso (como ID Scanner, sincronización de tarjetas, Guardtour y Morpho Biometrics)
g. Monitoreo de transacciones (POS, escaneo de códigos de barras y cajeros automáticos)
h. IoT Industrial (Modbus, BACnet, OPC, SNMP)
i. Industrial Protocol Interface (BACnet, Modbus)
j. Pared de video (Barco, Eizo)
k. Sistemas de administración de recursos humanos (HRMS)
l. Integración de Drones Autónomos
m. Teclas Inteligentes (Salto SVN, Medeco XT, CLIQ)
n. Detección de Disparos (Shot Spotter, Guardian GunShot)
o. Libro de Registro Dinámico
p. Plataforma de Reconocimiento Facial
q. Servicios de Localización en Tiempo Real - RTLS (HID)

2.33 Kit de desarrollo de software (SDK) de la USP

A. Un SDK de la USP deberá estar disponible para soportar el desarrollo personalizado para la plataforma.

B. El SDK deberá incluir funcionalidades específicas de los sistemas embebidos de reconocimiento automático de placas de matrícula (ALPR), control de acceso (ACS) y videos (VMS).

C. La integración con aplicaciones y bases de datos externas deberá ser posible con el SDK.

D. El SDK deberá permitir a los usuarios finales desarrollar nuevas funcionalidades (interfaz de usuario, aplicaciones o servicios independientes) para enlazar la USP a sistemas y aplicaciones empresariales de terceros como Sistemas para Uso de Emblemas, Sistemas de Administración de Recursos Humanos (HRMS), y sistemas de Planificación de Recursos Empresariales (ERP).

E. El SDK deberá basarse en la plataforma .NET.

F. El SDK deberá soportar actualizaciones dinámicas y transaccionales a la configuración de la USP. También deberá soportar el cambio de notificación de la configuración de entidad de la USP.

G. El SDK deberá proporcionar una lista completa de las funciones de programación para ver y/o configurar entidades básicas como lo son: usuarios y grupos de usuarios, alarmas, eventos personalizados, cronogramas. etc.

H. El SDK deberá proporcionar una lista completa de funciones de programación para ver y configurar el ACS, el VMS y el ALPR.

I. El SDK deberá proporcionar una lista completa de funciones de programación para ver y configurar la mayoría de las entidades ACS como: tarjetahabientes, grupos de tarjetahabientes, visitantes, credenciales, reglas de acceso (solo modificaciones) y campos personalizados.

J. El SDK deberá ser capaz de recibir eventos en tiempo real desde las siguientes entidades de la USP: usuarios y grupos de usuarios, áreas, zonas, cámaras, unidades de videos, puertas, controladores de puerta (unidades), elevadores, tarjetahabientes, grupos de tarjetahabientes y credenciales.

K. El SDK deberá ser capaz de consultar el historial de eventos para áreas, cámaras, zonas, alarmas, tarjetahabientes, credenciales, visitantes, puertas, eventos de lectura de consultas de placa de matrícula, eventos de aciertos de placas de matrícula automotriz, generar un informe de aciertos de placa de matrícula , generar un informe de lecturas de placa de matrícula.

L. El SDK deberá soportar las siguientes funciones de alarma: visualización de alarmas en tiempo real, reconocimiento de alarmas, cambiar prioridades y cambiar destinatario.

Parte 3 - Ejecución

3.01 Garantía

A. El producto deberá desarrollarse en todos los aspectos materiales de acuerdo con el manual del usuario adjunto, y los medios en donde resida el Software del Producto estarán libre de defectos en material y mano de obra bajo uso normal. Los defectos de software están cubiertos mediante Lanzamiento de Servicios y Actualizaciones Acumulativas las cuales están disponibles por un 1 año a partir de la fecha de la compra del software.

B. La garantía prolongada, hasta por 5 años, deberá estar disponible mediante la compra del contrato de mantenimiento de software (SMA) el cual incluye los siguientes servicios adicionales además de la garantía estándar:

1. Acceso a soporte telefónico y chat en línea para asistencia técnica.
2. Administración de caso en línea.
3. System Availability Monitor en línea.

4. Acceso a Actualizaciones de Versiones Importantes y Secundarias
5. Soporte de localizador las 24 horas, los 7 días de la semana y especialistas de soporte dedicados. *(Especificador: cargo adicional)*

3.02 Puesta en marcha del sistema y servicios de integración *(Especificador, este es un cobro diario más viáticos, revisar Genetec Inc. para ver el número recomendado de días a especificar)*

A. Requisitos Generales

1. El contratista deberá ocupar los servicios del integrador de la USP para asistir en la administración de la integración de la USP en el sitio del usuario final en proyectos que involucren:
    a. Varios contratistas o subcontratistas serán responsables por la integración de la USP en varios sitios del cliente en diferentes zonas geográficas.
    b. Las instalaciones empresariales complejas que involucran funcionalidades avanzadas (como la característica de Federation™, conmutaciones por error y plugins), sistemas múltiples (como control de acceso, videos y ALPR) o integraciones de terceros.
    c. El amplio uso de soluciones/plugins personalizados desarrollados por el integrador que se integrarán en la USP.
2. Los servicios del integrador de la USP deberán incluir la Administración de la Integración y Configuración y Puesta en Marcha del Sistema.

B. Servicio de Administración de Integración

1. El servicio de Administración de Integración del integrador deberá incluir un Gerente de Proyecto que actúa como el único punto de contacto para todas las comunicaciones entre el contratista y la organización del proveedor quién será el responsable de:
    a. Llevar a cabo la Evaluación de Riesgo del impacto sobre posibles factores de riesgo en el funcionamiento de la USP del integrador.
    b. Proporcionar un plan de proyecto para la integración de la USP del integrador.
    c. Administrar el desarrollo e implementación de los componentes de la solución personalizada que se integrarán a la USP del proveedor (si corresponde).
    d. Proporcionar un ámbito del trabajo que indique en detalle los servicios ofrecidos por el proveedor para asistir en la implementación de la USP del integrador.
    e. Coordinar y programar los servicios en campo del proveedor con el contratista para asistir en la implementación de la USP del proveedor.
    f. Proporcionar actualizaciones regulares del estado del proyecto al contratista en relación a la implementación de las soluciones personalizadas (si corresponde) y la implementación de la USP del proveedor.

C. Servicio de Arquitecto de Soluciones

1. El servicio de Arquitecto de Soluciones del proveedor deberá incluir un ingeniero de arquitectura de soluciones que actúe como único punto de contacto técnico durante la implementación de la USP y que será responsable de lo siguiente:

   a. Asistir al contratista/subcontratista con el diseño y la arquitectura de la USP del proveedor.

   b. Llevar a cabo actividades de consulta técnica que podrían incluir análisis de deficiencias/ajustes, revisiones de diseño del sistema, evaluaciones de compatibilidad de dispositivos, revisiones de diseño funcional y técnico, así como revisiones de rendimiento de la USP del proveedor.

   c. Realizar una evaluación del sistema y garantizar el cumplimiento de las mejores prácticas de la USP del proveedor.

   d. Proporcionar una estrategia de migración y actualización para la USP del proveedor según corresponda.

   e. Proporcionar documentación con relación a la arquitectura del sistema, el diseño del sistema, las especificaciones de hardware y los requisitos de compatibilidad, los cálculos del ancho de banda de las cámaras y las mejores prácticas con respecto a la USP del proveedor.

D. Configuración del Sistema y Servicio de Puesta en Marcha

1. La Configuración del Sistema y el Servicio de Puerta en Marcha del proveedor deberá incluir un Ingeniero de Campo quien será responsable por:

   a. Asistir a los técnicos en el lugar/remotos del contratista o subcontratista con la configuración y puesta en marcha de la USP del proveedor en el sitio del cliente.

   b. Llevar a cabo una prueba de la USP después de la instalación del sistema usando escenarios del operador reales para asegurar un desempeño óptimo del sistema.

   c. Proporcionar al contratista con un Informe de Servicio que indique con detalle las tareas realizadas durante la integración de la USP en el sitio del cliente, al igual que recomendaciones para mejorar el desempeño de la USP que deben ser implementadas por el contratista.

   d. Proporcionar una transferencia de conocimiento de la USP del proveedor al contratista después de la implementación de la USP en el sitio del cliente.

3.03 Capacitación del Fabricante para el Operador Usuario Final *(Especificador: Este es un cargo de medio día más gastos)*

A. El contratista deberá contratar los servicios del proveedor de la USP para asistir en la capacitación del usuario final de la USP en el sitio final del usuario.

Fin de Sección