ÍTEM 1 TORNIQUETE O CARRIL DE PASILLO BIDIRECCIONAL MEDIANAALTURA

<table>
<tr><td>Clasificación del bien o servicio</td><td>
<table>
<tr><th>Clasificación UNSPSC</th><th>Descripción</th></tr>
<tr><td>43211714</td><td>Equipos de Identificación Biométrica</td></tr>
<tr><td>46171619</td><td>Sistemas de seguridad o de control de acceso</td></tr>
<tr><td>72151701</td><td>Servicio de instalación de sistemas de control de acceso</td></tr>
<tr><td>72151704</td><td>Servicio de instalación de sistemas instrumentados de seguridad</td></tr>
</table>
</td></tr>
<tr><td>Nombre Comercial del Bien o Servicio</td><td>Torniquete o Carril Pasillo Bidireccional Mediana Altura</td></tr>
<tr><td>Calidad</td><td>CE, FCC, UL, RoHS.</td></tr>
<tr><td>Generalidades</td><td>Se requiere el suministro con implementación de un sistema de control de acceso que incluye barreras de acceso con tecnología de doble autenticación, facial y tarjeta que utilizan permite la autenticación mutua entre la tarjeta y el reconocimiento facial. Esta autenticación se realiza a través del envío de un mensaje.</td></tr>
<tr><td>Requisitos generales</td><td>El sistema de control de acceso debe permitir el paso bidireccional, controlando el ingreso y la salida de personas autorizadas en el sistema. Debe contar con doble factor de autenticación, que valide el primer factor mediante la lectura de tarjeta MIFARE Plus X4K para autenticación con credencial y el segundo factor mediante el lector de reconocimiento facial para autenticación biométrica.

El oferente deberá acreditar certificación vigente como integrador o partner autorizado por el fabricante de los equipos ofertados, que lo habilite para instalación y mantenimiento; se aceptaran certificaciones equivalentes emitidas por el fabricante o su canal de comercialización oficial en el país</td></tr>
<tr><td>Requisitos específicos</td><td>MOLINETE MEDIA ALTURA BIDIRECIONAL
Debe contar con fabricación para operación de alto tráfico
Acero inoxidable en Acero AISI 304 ó AISI 316
Debe contar con fabricación de uso en interiores.
Debe contar con puerta bidireccional en vidrio de 8mm ó 10 mm con función de liberación de puerta en caso de emergencia.
La altura de los vidrios debe ser entre 160cm a 180 cm.
Debe ser fabricado bajo diseño modular con cuerpos transparentes
Debe contar con una resistencia mecánica (MCBF) mínima de 12.000.000 de ciclos.
Fuente de potencia con capacidad de trabajar mínimo a 110 ó 240VAC 10 ó 220VAC.
Debe contar con motores bidireccionales con muy bajos umbrales de ruido, preferiblemente silenciosos.
El equipo debe contar con puerto ethernet para programación, configuración y mantenimiento
Debe contar con puertos de comunicación mínimo RS-232 ó RS-485 y TCP/IP.
Debe incluir soporte para la instalación de terminal de acceso con doble autenticación facial y tarjeta.
Debe contar con sistema de monitoreo remoto mediante conexión IP para mantenimiento, que permita la programación como barrera de entrada y salida con conteo digital, paso libre en las dos direcciones (ingreso y salida), fuera de servicio con bloqueo en las dos direcciones, antipánico que libre pasillo en caso de falta de fluido eléctrico o en caso de emergencia y activaciones de indicadores visuales que indiquen la disponibilidad del paso.
Debe contar con mecanismo de bloqueo automático, que impida el paso de persona no autorizada.
Debe contar con señalización inteligente a través pictogramas LED de mínimo dos colores dinámica (Para guía de tráfico peatonal)
Debe contar con un sistema de alarmas visibles y audibles.
Debe contar con pulsador de emergencia para permitir el paso libre en caso de una evacuación.
Debe contar con sensores de seguridad con la funcionalidad anti-colados y anti-atrapamiento o aplastamiento.
</td></tr>
</table>

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- El equipo debe contar con carta de garantía de fabrica que garantice la disponibilidad de repuestos durante 10 años.

Dimensiones de los pasillos

- Altura del cuerpo entre 92cm y 99 cm.
- Ancho de carril para paso peatonal 60cm
- Ancho de carril para paso personas en condición de movilidad reducida 90cm
- Altura del vidrio entre 160cm y 180Cm de alto
- Verificar la distancia en la visita técnica



Imagen de Ref.

FUENTE DE POTENCIA PARA TARJETAS CONTROLADORAS DE ACCESO

Características técnicas mínimas:

Capacidad	Debe tener capacidad para alimentar y alojar las tarjetas controladoras de acceso
Fuente de alimentación	Debe contar con fuente de alimentación doble, con capacidad de conexión de 110v o 220v
Salida potencia	Debe contar con salida de potencia mínima de 140W a 12v ó 24v con 16 salidas cableadas. Debe contar con salida de potencia mínima de 240W a 12v ó 24v con cargadores de baterías cableados
Gabinete	Debe estar fabricado en acero pintado y contar con cerradura de llave, sensor de apertura de puerta
Compatibilidad	Debe ser compatible para instalar tarjetas controladoras principales IP para control de acceso y tarjetas expansoras de control de acceso.
Placa	Debe contar con placa trasera perforada con separadores y tornillos para la instalación de tarjetas de acceso.
Software y accesorios	Debe incluir los accesorios necesarios para su correcta instalación y funcionamiento. Debe incluir el cableado de comunicaciones necesario para la puesta en funcionamiento.
Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
Accesorio o dispositivo	De ser necesario para su perfecto funcionamiento y compatibilidad con los dispositivos del sistema deberá ser suministrado por el proveedor.
Batería	Debe contar con mínimo 02 baterías para autonomía de mínima de 2 horas en caso de falta de energía.
Garantía de fabricación	Mínima Dos (02) años

TARJETA EXPANSORA DE CONTROL DE ACCESO

Características técnicas mínimas:

Marca	N/A
Modelo o referencia	N/A
Expansión	Debe contar con integración nativa con la Tarjeta controladora principal IP para control de acceso y

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		ampliar la lectura y control de hasta 2 terminales de control de acceso.
	Capacidad de control	De mínimo 02 terminales de lectura
	Alimentación de energía	12Vdc ó 24Vd ó POE
	Conectividad	Mínimo OSDP y RS485
	Entradas	Mínimo 06 entradas
	Salidas	Mínimo 04 salidas con relevos
	Seguridad	Debe tener la capacidad de comunicación protegida por TLS ó mínimo AES 128 ó 256 o FIPS 140-3
	Protocolos	Debe Soportar Protocolos OSDP, RS485 y Wiegand.
	Funcionalidades mínimas	Debe soportar múltiples terminales de autenticación para control de acceso en barreras de acceso.
	Indicador	Debe contar con LED indicador de estado
	Capacidad de control puertas o molinete	Debe tener la capacidad de administrar mínimo 1 puerta o molinete mediante lector biométrico ingreso – lector biométrico salida
	Temperatura de operación	Debe tener la capacidad de funcionar a mínimo 0° hasta 68°C.
	Certificaciones	CE, FCC, RoHS, UL.
	Húmeda de funcionamiento	Entre 5 a 95% sin condensación
	Compatibilidad	Debe ser asegurada con el fabricante de software control de acceso ofertado y la Tarjeta controladora principal IP para control de acceso ofertada.
	Software y accesorios	Debe incluir los accesorios necesarios para su correcta instalación y funcionamiento. Debe incluir el cableado de comunicaciones compuesto necesario para la puesta en funcionamiento.
	Soporte	El proponente debe adjuntar carta del fabricante que le habilite como canal certificado y con experiencia para la comercialización y el soporte de la solución ofertada en el territorio colombiano
	Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
	Accesorio o dispositivo	De ser necesario para su perfecto funcionamiento y compatibilidad con los dispositivos del sistema deberá ser suministrado por el proveedor.
	Garantía de fabricación	Mínima Dos (02) años
	Deberán suministrar los accesorios requeridos para el funcionamiento sin ningún costo adicional para el correcto funcionamiento	
Empaque y rotulado	No requiere empaque y/o rotulado especial	
Presentación y Unidad de Medida	Unidad	
Cantidad	16	

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

ÍTEM 2 TORNIQUETE BIDIRECIONAL ALTURA COMPLETA

<table>
<tr><td>Clasificación del bien o servicio</td><td>
<table>
<tr><th>Clasificación UNSPSC</th><th>Descripción</th></tr>
<tr><td>43211714</td><td>Equipos de Identificación Biométrica</td></tr>
<tr><td>46171619</td><td>Sistemas de seguridad o de control de acceso</td></tr>
<tr><td>72151701</td><td>Servicio de instalación de sistemas de control de acceso</td></tr>
<tr><td>72151704</td><td>Servicio de instalación de sistemas instrumentados de seguridad</td></tr>
</table>
</td></tr>
<tr><td>Nombre Comercial del Bien o Servicio</td><td>Torniquete Bidireccional Altura Completa</td></tr>
<tr><td>Calidad</td><td>CE, FCC, UL, RoHS.</td></tr>
<tr><td>Generalidades</td><td>Se requiere el suministro con instalación de torniquete de altura completa para alta seguridad que permita la implementación y autenticación mutua entre la tarjeta y el reconocimiento facial para permitir el cruce de la persona autenticada.</td></tr>
<tr><td>Requisitos generales</td><td>El sistema debe permitir el paso bidireccional, controlando el ingreso y la salida de personas. Debe contar con doble factor de autenticación, que combine: Lector de tarjeta MIFARE Plus X4K para autenticación con credencial, Módulo de reconocimiento facial para autenticación biométrica.
El equipo molinete de altura completa debe contar con carta de garantía de fabrica que garantice la disponibilidad de repuestos durante 10 años.

El oferente deberá acreditar certificación vigente como integrador o partner autorizado por el fabricante de los equipos ofertados, que lo habilite para instalación y mantenimiento; se aceptarán certificaciones equivalentes emitidas por el fabricante o su canal de comercialización oficial en el país.</td></tr>
<tr><td>Requisitos específicos</td><td>

Debe estar fabricado en acero inoxidable AISI 304 ó AISI 316.
Debe contar con fabricación para operación de alto tráfico.
El equipo debe estar fabricado para uso en exteriores con mecanismo de rotación bidireccional mediante motor sin escobillas.
Fuente de potencia con capacidad de trabajar mínimo a 110 ó 220VAC.
El equipo debe contar con certificación RETIE en Colombia.
El equipo debe contar con sensores para la detección de personas durante el paso que permita evitar colados.
Puertos de comunicación (RS-232 ó RS-485 y TCP/IP)
Debe contar con señalización inteligente a través pictogramas LED (Para guía de tráfico peatonal)
Debe contar con una resistencia mecánica (MCBF) mínima de 12.000.000 de ciclos
Debe contar con pulsador de emergencia para permitir el paso libre en caso de una evacuación.
El equipo debe contar con carta de garantía de fabrica que garantice la disponibilidad de repuestos durante 10 años.
Dimensiones de los molinetes de altura completa
Alto entre 225 y 235cm; ancho entre 150 a 165cm; Profundidad 130cm y 150cm
Verificar la distancia en la visita técnica


Imagen de Referencia

FUENTE DE POTENCIA PARA TARJETAS CONTROLADORAS DE ACCESO
</td></tr>
</table>

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Características técnicas mínimas:

Capacidad	Debe tener capacidad para alimentar y alojar las tarjetas controladoras de acceso
Fuente de alimentación	Debe contar con fuente de alimentación doble, con capacidad de conexión de 110v o 220v
Salida potencia	Debe contar con salida de potencia mínima de 140W a 12v ó 24v con 16 salidas cableadas. Debe contar con salida de potencia mínima de 240W a 12v ó 24v con cargadores de baterías cableados
Gabinete	Debe estar fabricado en acero pintado y contar con cerradura de llave, sensor de apertura de puerta
Compatibilidad	Debe ser compatible para instalar tarjetas controladoras principales IP para control de acceso y tarjetas expansoras de control de acceso.
Placa	Debe contar con placa trasera perforada con separadores y tornillos para la instalación de tarjetas de acceso.
Software y accesorios	Debe incluir los accesorios necesarios para su correcta instalación y funcionamiento. Debe incluir el cableado de comunicaciones necesario para la puesta en funcionamiento.
Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
Accesorio o dispositivo	De ser necesario para su perfecto funcionamiento y compatibilidad con los dispositivos del sistema deberá ser suministrado por el proveedor.
Batería	Debe contar con mínimo 02 baterías para autonomía de mínima de 2 horas en caso de falta de energía.
Garantía de fabricación	Mínima tres (03) años

TARJETA CONTROLADORA DE CONTROL DE ACCESO

Características técnicas mínimas:

Marca	N/A
Modelo o referencia	N/A
Expansión	Debe contar con integración nativa con la Tarjeta controladora principal IP para control de acceso y ampliar la lectura y control de hasta 2 terminales de control de acceso.
Capacidad de control	De mínimo 02 terminales de lectura
Alimentación de energía	12Vdc ó 24Vd ó POE
Conectividad	Mínimo OSDP y RS485
Entradas	Mínimo 06 entradas
Salidas	Mínimo 04 salidas con relevos
Seguridad	Debe tener la capacidad de comunicación protegida por TLS ó mínimo AES 128 ó 256 ó FIPS 140-3
Protocolos	Debe Soportar Protocolos OSDP, RS485 y Wiegand.
Funcionalidades mínimas	Debe soportar múltiples terminales de autenticación para control de acceso en barreras de acceso.
Indicador	Debe contar con LED indicador de estado
Capacidad de control puertas o molinete	Debe tener la capacidad de administrar mínimo 1 puerta o molinete mediante lector biométrico ingreso – lector biométrico salida
Temperatura de operación	Debe tener la capacidad de funcionar a mínimo 0° hasta 68°C.
Certificaciones	CE, FCC, RoHS, UL.
Húmeda de	Entre 5 a 95% sin condensación

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	funcionamiento	
	Compatibilidad	Debe ser asegurada con el fabricante de software control de acceso ofertado y la Tarjeta controladora principal IP para control de acceso ofertada.
	Software y accesorios	Debe incluir los accesorios necesarios para su correcta instalación y funcionamiento. Debe incluir el cableado de comunicaciones compuesto necesario para la puesta en funcionamiento.
	Soporte	El proponente debe adjuntar carta del fabricante que le habilite como canal certificado y con experiencia para la comercialización y el soporte de la solución ofertada en el territorio colombiano
	Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
	Accesorio o dispositivo	De ser necesario para su perfecto funcionamiento y compatibilidad con los dispositivos del sistema deberá ser suministrado por el proveedor.
	Garantía de fabricación	Mínima Dos (02) años
Empaque y rotulado	No requiere empaque y/o rotulado especial	
Presentación y Unidad de Medida	Unidad	
Cantidad	04	

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

ÍTEM 3 TERMINAL DE ACCESO CON DOBLE AUTENTICACIÓN FACIALY TARJETA

Clasificación del bien o servicio	<table><tr><th>Clasificación UNSPSC</th><th>Descripción</th></tr><tr><td>43211714</td><td>Equipos de Identificación Biométrica</td></tr><tr><td>46171619</td><td>Sistemas de seguridad o de control de acceso</td></tr><tr><td>72151701</td><td>Servicio de instalación de sistemas de control de acceso</td></tr><tr><td>72151704</td><td>Servicio de instalación de sistemas instrumentados de seguridad</td></tr></table>
Nombre Comercial del Bien o Servicio	Terminal de acceso con doble autenticación facial y tarjeta
Calidad	CE, FCC, RoHS, UL.
Generalidades	Se requiere el suministro con implementación de un sistema de control de acceso que permita la autenticación mutua entre la tarjeta y el reconocimiento facial. El sistema debe contar con el licenciamiento necesario y equipos para la puesta en funcionamiento de acuerdo con la marca ofertada.
Requisitos generales	El sistema de control de acceso debe permitir el **paso bidireccional**, controlando el ingreso y la salida de personas autorizadas en el sistema. Debe contar con **doble factor de autenticación**, que valide el primer factor mediante la lectura de **tarjeta MIFARE Plus X4K** para autenticación con credencial y el segundo factor mediante el lector de **reconocimiento facial** con IA para autenticación biométrica. El oferente deberá acreditar certificación vigente como integrador o partner autorizado por el fabricante de los equipos ofertados, que lo habilite para instalación y mantenimiento; se aceptarán certificaciones equivalentes emitidas por el fabricante o su canal de comercialización oficial en el país.
Requisitos específicos	Autenticación facial y tarjeta **MIFARE Plus X4K** para acceso y salida por cada molinete • El funcionamiento del sistema control de acceso debe permitir validar mediante con tarjeta y biometría facial. • El sistema debe contar con terminales de reconocimiento facial que realice la autenticación facial mediante cámara de mínimo 2mpx y con iluminador infrarrojo motorizado. • La biometría facial debe contar con tecnología de identificación de detección de imagen de persona viva que permita negar el acceso a rostros simulados, fotografías, videos. • El equipo debe contar con certificación ISO/IEC 27001 que permita proteger la seguridad de la información de los funcionarios de la FGN. • Debe permitir trabajar con fuente de alimentación a 12V ó 24V ó POE • Debe contar con la capacidad de compartir video por medio de protocolo Onvif ó RTSP. • Debe tener la capacidad de almacenar mínimo 50.000 plantillas faciales, y capacidad de autenticación de 1 plantilla facial en máximo en 0,5 segundos. • La terminal facial debe contar con tecnología que permita a la terminal resistir a manipulaciones y proteger los datos sensibles como claves y biometría. • La terminal debe contar mínimo un puerto ethernet a 1000Mbps. • Debe permitir el reconocimiento facial entre 10 cm y 100cm de distancia para el reconocimiento y autenticación y apertura. • Debe contar con una pantalla LCD con tamaño entre 4,5´´ y 5,5´´. • Debe contar con puertos de comunicación RS-232 ó RS 485, OSDP y Wiegand. • La terminal de control de acceso debe contar con lector para tarjetas MIFARE PLUS X4K para doble autenticación para acceso y salida por cada molinete integrado a la plataforma de control de acceso con todos los accesorios necesarios. • El oferente debe incluir en la oferta todos los accesorios, controladores y licencias de software necesario para la instalación y puesta en funcionamiento. • Garantía mínima por defectos de fábrica de 2 años.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Empaque y rotulado	No requiere empaque y/o rotulado especial
Presentación y Unidad de Medida	Unidad
Cantidad	43

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

ÍTEM 4 EQUIPO SERVIDOR PARA ADMINISTRACIÓN Y GESTIÓN DE CONTROL DE ACCESO

<table>
<tr><td>Clasificación del bien o servicio</td><td>
<table>
<tr><th>Clasificación UNSPSC</th><th>Descripción</th></tr>
<tr><td>43211714</td><td>Equipos de Identificación Biométrica</td></tr>
<tr><td>46171619</td><td>Sistemas de seguridad o de control de acceso</td></tr>
<tr><td>72151701</td><td>Servicio de instalación de sistemas de control de acceso</td></tr>
<tr><td>72151704</td><td>Servicio de instalación de sistemas instrumentados de seguridad</td></tr>
</table>
</td></tr>
<tr><td>Nombre Comercial del Bien o Servicio</td><td>Equipo servidor para administración y gestión de control de acceso.</td></tr>
<tr><td>Calidad</td><td>CE, FCC, RoHS, UL</td></tr>
<tr><td>Generalidades</td><td>Se requiere el suministro con implementación de un equipo servidor de para administración y gestión de control de acceso, con la configuración y puesta en funcionamiento de acuerdo con la marca ofertada.</td></tr>
<tr><td>Requisitos generales</td><td>El equipo servidor de para administración y gestión de control de acceso debe tener la capacidad de procesar la administración del sistema de control de acceso para mínimo terminales de lectura y mínimo 200.000 identidades.
Certificación del fabricante al oferente como empresa certificada en instalación y mantenimiento de los equipos ofertados.

El oferente deberá acreditar certificación vigente como integrador o partner autorizado por el fabricante de los equipos ofertados, que lo habilite para instalación y mantenimiento; se aceptaran certificaciones equivalentes emitidas por el fabricante o su canal de comercialización oficial en el país.</td></tr>
<tr><td>Requisitos específicos</td><td>Características técnicas mínimas:
<table>
<tr><td>Marca</td><td>N/A</td></tr>
<tr><td>Modelo o referencia</td><td>N/A</td></tr>
<tr><td>Hardware</td><td>En este dispositivo se instalará el software de gestión y administración de control de acceso tipo corporativo con integración a sistema de video seguridad</td></tr>
<tr><td rowspan="2">Montaje</td><td>Tipo rack</td></tr>
<tr><td>Máximo 2U de rack de 19”</td></tr>
<tr><td>Procesador</td><td>Un (01) Procesador Intel Xeon E-2330 o Superior</td></tr>
<tr><td>Velocidad de bus</td><td>8 Gt/s</td></tr>
<tr><td>Memoria Ram</td><td>Mínimo 16 GB DDR4 ó DDR5</td></tr>
<tr><td>Almacenamiento</td><td>Mínimo 2Tb</td></tr>
<tr><td>Tipo de discos para almacenamiento</td><td>Discos SATA, SAS o NL-SAS tipo Enterprise para servidores</td></tr>
<tr><td>Capacidad de procesos por minuto</td><td>Debe tener la capacidad de procesar mínimo 48.000 transacciones de acceso por minuto</td></tr>
<tr><td>Conexión ethernet</td><td>El servidor debe tener mínimo 02 conexiones o puertos Ethernet a 1000Mbps

Puerto dedicado de administración remota out-of-band compatible con estándares IPMI 2.0 o equivalente”</td></tr>
<tr><td>Temperatura de operación</td><td>10°C a 35°C o mejor.</td></tr>
<tr><td>Periféricos</td><td>Ratón y teclado</td></tr>
<tr><td>Lector</td><td>CD-RW / DVD-RW: Interna o externa</td></tr>
<tr><td>Capacidad de</td><td>Debe tener la capacidad de administrar mínimo 380</td></tr>
</table>
</td></tr>
</table>

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

procesar puertas	puertas
Puerto de video	Mínimo 1x VGA o 1x HDMI
Altura de operación	El servidor deberá tener la capacidad de funcionar a mínimo 3.000. metros de altura.
Certificaciones	CE, FCC, RoHS, UL
Húmeda de funcionamiento	Entre 5 a 80% sin condensación
Fuente de energía	Con capacidad de trabajar 110 y 220 Vac
Licencias	Licencias: Sistema operativo preinstalado en fábrica, mínimo Windows o similar.
Compatibilidad	Asegurada con el fabricante de Software control de acceso
Software y accesorios	Para configuración e instalación
Máximo consumo de potencia	500W o menor
Soporte	Servicio de soporte y reparaciones en sitio durante el tiempo de garantía de fábrica (Sin costo adicional), incluir certificación expedida por el fabricante.
	El proponente debe adjuntar carta del fabricante que le habilite como canal certificado y con experiencia para la comercialización y el soporte de la solución ofertada en el territorio colombiano
Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
Accesorio o dispositivo	De ser necesario para su perfecto funcionamiento y compatibilidad con los dispositivos del sistema deberá ser suministrado por el proveedor.
Garantía de fabrica	Mínima tres (02) años

CARACTERÍSTICAS MÍNIMAS DE SOFTWARE DE GESTIÓN Y ADMINISTRACIÓN DE CONTROL DE ACCESO TIPO CORPORATIVO CON INTEGRACIÓN A SISTEMA DE VIDEO SEGURIDAD

El sistema, debe permitir realizar gestión avanzada de alarmas e identidades de forma fácil y flexible en el sistema para proporcionar un control eficiente de acceso a nuestras instalaciones.
El software debe de funcionar sin interrupciones de forma completa en los diferentes navegadores web de la industria, sin que tengamos limitantes a la hora de realizar gestión, administración o simplemente responder de forma rápida alertas desde cualquier lugar.
El software de control de acceso debe contar con integración con el sistema de video existente en la Fiscalía General de la Nación marca Avigilon Interprise, para revisar y verificar las alarmas que se puedan generar en ambos sistemas de forma automática vinculando el evento al momento exacto de video en vivo como grabado para control rápido y respuesta eficiente. Sin costo adicional.
Se requiere que el sistema se pueda configurar bajo en un plano de la Fiscalía general de la nación donde se ubique visualmente la puerta o elemento a monitorear y a su vez se pueda realizar un bloqueo/desbloqueo remoto de puertas incluso en estado de alarma. Sin costo adicional.
Con la integración al sistema de video, la plataforma debe permitir realizar una búsqueda por el nombre de una identidad, los resultados obtenidos sean el momento exacto de video de cuando alguien intento ingresar por una puerta especifica al realizar la marcación correspondiente, de esta manera si se tiene una cámara cerca a la puerta en cuestión, se tenga evidencia fiel de que la persona que ingreso, lo hizo con su propia credencial de acceso. Sin costo adicional.
Se requiere que el sistema opere con Hardware de terceros que este homologado o certificado para trabajar con diferentes marcas de software en la industria, para evitar limitación en implementación y garantizar una estructura de plataforma abierta.
En caso de falla, el sistema deberá contar con la posibilidad de realiza replicación de bases de datos de identidades del sistema completo en varios dispositivos de forma automática por error en

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	modo de espera activa de los dispositivos para contar con varios niveles de redundancia y resistencia a fallos.
	La operación del hardware de campo no debe depender de la operación del servidor de aplicación puesto que, en caso de una falla total del sistema, el sistema de control de acceso debe permanecer operativo.
	El sistema de control de acceso debe integrarse al sistema de video seguridad (CCTV) existente en el Bunker Fiscalía general de la nación sin necesidad de licencias adicionales.
	Debe proporcionar las facilidades para la verificación de video, combinando el sistema de control de acceso con las cámaras de CCTV ya instaladas en las instalaciones de la Fiscalía general de la nación Nivel central Bunker.
	Toda la configuración, el mantenimiento y la interacción con el sistema, se debe obtener sin la interacción con el sistema operativo o la estructura de directorios.
	La interfaz de trabajo y configuración de la plataforma de control de acceso deberá ser únicamente vía navegador web, sin la necesidad de requerir una estación de trabajo dedicada. Como mínimo deberá el sistema ser capaz de soportar los siguientes navegadores web: Mozilla Firefox, Google Chrome, Apple Safari.
	Es imperativo garantizar la estabilidad operativa del servidor y la integridad de la comunicación interna (back-end), minimizando los cuellos de botella en el flujo de datos local.
	La plataforma de control de acceso deberá soportar como mínimo, pero no solo estar limitado al siguiente hardware de campo (controladores y subcontroladores) para control de acceso compatibles con al menos 10 diferentes fabricantes, dentro de los cuales deben estar como mínimo la línea de Producto de Mercury Security series 1, 2 y 3, línea de producto de HID Global VertX EVO, línea de producto Salto Systems: Unidad de control CU42E0US y CU4200US.
	La plataforma deberá soportar medidas de seguridad para todas las comunicaciones e información de la solución soportando como mínimo SSL 128 bit de encripción o superior.
	Debe contar con software de monitoreo y gestión que permite administrar de manera centralizada diversas los diferentes controladores que hagan parte del sistema integrado de control de acceso, además te permitir la interacción con el sistema de video de forma integrada.
	La plataforma de control de acceso deberá tener inmersa la funcionalidad de administrar y gestionar multi-sitios.
	El software gestión y administración de control de acceso tipo corporativo con integración a sistema de video seguridad debe tener la capacidad de soportar 2048 lectores, y soportar hasta 512 controladores, (50) operadores simultáneos (a través del navegador), sin costo adicional.
	Debe ser suministrado el licenciamiento de administración de control de acceso (a perpetuidad) para instalación en para administración y gestión de control de acceso para mínimo 116 lectores.
	Debe tener la capacidad de integrarse con las siguientes bases de datos de terceros estándar de la industria, Bidireccional: • Protocolo ligero de acceso a directorios (LDAP/Active Directory). • SQL. • Sistema de gestión de bases de datos relacionales de Oracle. • Valor separado por comas (CSV). • Lenguaje de marcado extensible (XML).
	Deber permitir integraciones personalizadas usando Rest API
	Debe contar con una interfaz de usuario de uso intuitivo que permita ver las siguientes funcionalidades sin limitarse a ellas: • Supervisar eventos, alarmas y estado del hardware en tiempo real. • Verificar identidades en tiempo real. • Buscar eventos históricos y alarmas.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	Debe permitir la configuración de funcionalidades tales como: • Grupos de acceso: Capacidad de crear grupos de terminales de acceso y horarios de modo que las terminales puedan permitir o restringir el acceso a áreas según los horarios. • Registros de Identidad: Proporcionar un sistema con gestión de identidad integrada, permitiendo la importación de datos desde bases de datos soportadas. Cada identidad admite el control de acceso basado en grupos y roles, así como anulaciones individuales. Incluya funcionalidad para personalizar formularios de identidad y token en el software base. Proporcionar registros de identidad capaces de gestión y sincronización entre múltiples sitios. • Roles: Debe tener un método de permiso basado en roles que permite asignar uno o más roles a las identidades para determinar el acceso físico y lógico. • Anti-Passback: Proporcionar un software de control de acceso capaz de designar áreas para requerir una autenticación para ingresar y salir del área antes de que se use para ingresar al área nuevamente. o APB de área suave y dura: realiza un seguimiento de cada credencial que ingresa a un área específica y define a qué áreas puede acceder la credencial a continuación. o APB basado en puerta: realiza un seguimiento de cada credencial que ingresa y no permite que la misma credencial ingrese dos veces seguida hasta que se alcanza el límite de tiempo de APB. o APB cronometrado basado en tokens: realiza un seguimiento de cada puerta a la que ha accedido un distintivo. Después de que la insignia haya accedido a una puerta, debe acceder a una segunda puerta o esperar hasta que se alcance el límite de tiempo de APB antes de poder acceder a la primera puerta nuevamente. o APB de área temporizada: APB de área dura basada en tiempo. Cuando expira el límite de tiempo, el área dura APB se convierte en un área blanda APB. o Hard Door APB: rastrea cada credencial que ingresa a una puerta y no permite que la misma credencial ingrese dos veces seguida. o Soft Door APB: rastrea cada credencial que ingresa a una puerta y genera una transacción de advertencia si la misma credencial se usa en la misma puerta dos veces seguidas. • Macros: Debe proporcionar un sistema capaz de vincular uno o más eventos a macros de modo que un solo evento pueda ejecutar hasta 30 macros. El sistema debe admitir un mínimo de 255 macros por controlador de campo inteligente. • Encryption: Debe proporcionar un sistema de control de acceso que admita los siguientes métodos de cifrado: o TLS 1.2: requiere cifrado TLS entre el sistema de control de acceso y el controlador ofertado. o Certificados personalizados: requiere un certificado de autoridad certificadora o auto firmado para fortalecer el sistema de control de acceso. Los certificados autenticarán los controladores ofertados en el sistema de control de acceso.
	La plataforma debe contar con un Dashboard • Debe permitir la creación de un tablero para el estado y las acciones en tiempo real de los componentes de hardware en una sola pantalla que también puede filtrar por nombre, estado, dispositivo o grupo. 1. o Estado del hardware: Controladores: Comunicación, potencia, sabotaje y batería. Subcontroladores: comunicación, alimentación y manipulación. Entradas: inactiva, activa, problema y enmascarada. Salidas: Apagado, encendido y problema. Puertas: Comunicación, sabotaje, batería, desbloqueo, ayuda, enmascarado y forzado. Dispositivos: RAM, programa, base de datos, carga de CPU y estado del puerto. o Supervisar:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	Paneles: estado del dispositivo, estado de seguridad, nombre, modelo, firmware, dirección IP, dirección MAC, tarjetas en uso y última comunicación. Paneles secundarios: estado del dispositivo, nombre, panel, tipo, puerto, dirección y firmware. Entradas: estado del dispositivo, nombre de entrada, subpanel, resistencia EOL y dirección. Salidas: estado del dispositivo, nombre de salida, subcontrolador, programación y dirección. Fuentes de alimentación: nombre de la fuente de alimentación, estado de instalación, estado y registros. Puertas de control de acceso: estado, nombre, panel, estado de la puerta, modo de puerta y estado de anulación. o Manipular puertas de control de acceso: Acciones de la puerta: Otorgar, restaurar, desbloquear, bloquear sin acceso, deshabilitar.
	Debe contar con una estación de verificación virtual, esta debe proporcionar una conexión habilitada para navegador web al software de control de acceso para permitir que un usuario confirme visualmente la identidad y la autorización de una persona que intenta ingresar a un área de control.
	Debe permitir coincidencia de servidores, registros de video, de imágenes y seguimientos para auditoría.
	La plataforma debe contar con una Interfaz de mapa: • Deberá proporcionar una interfaz para crear diseños personalizables que incluyan planos de planta, ubicaciones de lectores y botones que pueden desencadenar acciones. o Acciones: Indicar la alarma mediante un icono, deshabilitar, desbloquear, bloquear, otorgar, restaurar, enmascarar retenido, desenmascarar retenido y rastrear acciones. o Ocupación/reunión: los mapas proporcionarán la ocupación en tiempo real de un área definida. o Botones programables: Proporcionar mapas de botones y texto para realizar acciones.
	Soporte remoto: • La plataforma deberá tener la capacidad de soporte remoto para permitir el acceso para soporte técnico y de ingeniería de personal certificado en el software para: o Solución de problemas o Diagnósticos o Carga del Sistema o Asistencia con la configuración. Deberá tener la capacidad de obtener datos de registro del log de eventos del software para obtener un mejor soporte de la aplicación.
	Replicación basada en cuadrícula: • La plataforma deberá admitir la arquitectura de replicación basada en cuadrícula automatizada de la estructura de directorios del dispositivo para implementar múltiples dispositivos. o La arquitectura de replicación debe ser de igual a igual y no requiere un servidor de base de datos dedicado para permitir la replicación de identidades y datos de configuración en todos los dispositivos. o Deberá admitir comunicaciones cifradas entre dispositivos utilizando cifrado SSL. o La replicación deberá permitir que los datos LDAP de todos los dispositivos se sincronicen con cada uno de los otros en el sistema, permitiendo que el dispositivo se reconstruya a partir de los datos replicados encontrados en otro dispositivo del sistema.
	Funcionalidad Hot Standby: • Debe ser compatible con una arquitectura de hot standby y conmutación por error. o Para cada dispositivo, un dispositivo Hot Standby se deberá configurar para monitorear el estado de su dispositivo asociado principal. En caso de que un dispositivo no funcione, el dispositivo de espera activa debe ser capaz de detectar automáticamente un problema y asumir el control del sistema.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	Actualizaciones de software: • La plataforma deberá admitir actualizaciones mediante la descarga desde el sitio web del fabricante o la recepción por correo electrónico de los archivos de actualización. No se deberá requerir interacción física con el dispositivo control de acceso para realizar una actualización exitosa del software del sistema.

	Respaldos del sistema:
	• Deberá tener la capacidad de respaldar y restaurar la estructura de directorios de LDAP.
	  ○ Las copias de seguridad deberán ejecutarse simultáneamente con el resto del sistema y no requerirán que todos los operadores se desconecten del servidor de control de acceso.
	  ○ Las copias de seguridad deben incluir datos de transacción y datos de configuración del sistema.
	  ○ Las copias de seguridad del dispositivo se pueden cifrar mediante el cifrado AES.
	  ○ Copias de seguridad del dispositivo para:
	  ▪ Dispositivo de almacenamiento USB
	  ▪ Directorio compartido de Windows o carpeta compartida de red
	  ▪ Servidores SCP
	  ○ Las copias de seguridad se realizarán:
	  ▪ Automáticamente en un horario diario predefinido
	  ▪ Manualmente a través de la interfaz de usuario.

	Deberá soportar como mínimo los siguientes idiomas en su interfaz gráfica a. Ingles b. Español
	Plataforma software. a. Debe tener la capacidad de configurar mínimo 60 días feriados b. Debe tener la capacidad de crear mínimo 60 grupos de accesos c. Debe tener la capacidad de generar mínimo 200 zonas de tiempo d. Debe tener la capacidad de gestión de dispositivos con tecnología Wiegand u OSDP e. Debe generar mapas que permiten visualizar las ubicaciones de puntos de control de acceso y el estado f. Debe permitir la configuración de antipassback a todo el sistema
	La plataforma deberá tener dentro de sus atributos: La capacidad de control de parqueaderos. Integración con plataformas de video seguridad.
	El proponente junto con la oferta deberá adjuntar carta directa de la casa fabricante que lo certifique como empresa integradora certificada, vendedora autorizada y proveedor para el soporte de la marca del sistema de control de acceso ofertado. (No se aceptarán carta de distribuidores mayoristas).
	La plataforma de control de acceso debe contar con las funcionalidades desde dispositivos móviles que permita otorgar acceso, bloquear/desbloquear puertas, ver el estado de la puerta en tiempo real, actualizar el estado del acceso o activar un bloqueo en todo el sitio.
	La plataforma de control de acceso debe tener la funcionalidad de escenas con un enfoque dinámico para gestionar objetos de seguridad desde una vista personalizable en tiempo real.
	Debe contar con la funcionalidad de escenas y permitir localizar visualmente dónde se encuentran las puertas, cámaras, entradas y salidas en sus instalaciones. Debe permitir utilizar cualquier imagen en archivos BMP, GIF, JPEG, PNG o PDF. Las escenas deben permitir mostrar elementos del panel de control de áreas, incluidas las áreas de reunión.
	La funcionalidad de escenas deberá permitir el bloqueo o desbloqueo de puertas de un sitio.
	La plataforma debe contar con la funcionalidad recopilación de identidades que permitan rastrear en el software de manera interactiva datos en tiempo real, que permite la rápida identificación del personal que falta en caso de una evacuación de emergencia.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	La plataforma de control de acceso debe contar con la funcionalidad de alarmas de manera optimizada, que permita gestionar las alarmas reconocidas, no reconocidas y las programadas. Debe ser basado en roles, que definan el acceso físico y lógico de un usuario en función de roles que normalmente están asociados con un grupo de identidades. Debe contar con una solución de credenciales integrada que permita diseñar e imprimir credenciales desde el navegador de la plataforma. Debe permitir la funcionalidad de reportes pre-existentes así mismo debe permitir personalizar informes para mostrar datos importantes de control de acceso adecuados a la medida para la Fiscalía General de la Nación. Debe contar con una herramienta de apoyo a la toma de decisiones intuitiva y basada en la nube, diseñada para mejorar la eficiencia en varios sitios; debe permitir agilizar los informes de incidentes y permitir que los equipos de seguridad sean más ágiles y productivos mediante una interfaz de pantalla única que unifica el video, el control de acceso y una respuesta a incidentes estructurada y personalizada. La integración con la plataforma y la herramienta de apoyo a la toma de decisiones basada en la nube, no debe requerir de un gateway cloud externo. Debe contar con la funcionalidad o programa de software basado en la nube que unifique las soluciones de seguridad en una herramienta de automatización del flujo de trabajo intuitiva. Debe contar con la certificación mínimo dos de las siguientes certificaciones, NDAA, ISO27001.
Empaque y rotulado	No requiere empaque y/o rotulado especial
Presentación y Unidad de Medida	Unidad
Cantidad	1

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

ÍTEM 5 TARJETA CONTROLADORA PRINCIPAL IP PARA CONTROL DE ACCESO

<table>
<tr><td>Clasificación del bien o servicio</td><td>
<table>
<tr><th>Clasificación UNSPSC</th><th>Descripción</th></tr>
<tr><td>43211714</td><td>Equipos de Identificación Biométrica</td></tr>
<tr><td>46171619</td><td>Sistemas de seguridad o de control de acceso</td></tr>
<tr><td>72151701</td><td>Servicio de instalación de sistemas de control de acceso</td></tr>
<tr><td>72151704</td><td>Servicio de instalación de sistemas instrumentados de seguridad</td></tr>
</table>
</td></tr>
<tr><td>Nombre Comercial del Bien o Servicio</td><td>Tarjeta controladora principal IP para control de acceso</td></tr>
<tr><td>Calidad</td><td>CE, FCC, RoHS, UL, NIST</td></tr>
<tr><td>Generalidades</td><td>Se requiere el suministro con implementación de tarjetas controladoras principales de acceso IP como interfaz de control entre las terminales biométricas, permisos de acceso configurados en el software de control de acceso.</td></tr>
<tr><td>Requisitos generales</td><td>Se requiere el suministro con implementación de tarjetas controladoras principales de acceso IP conectadas al software de acceso instalado en el servidor de para administración y gestión de control de acceso, que permita controlar las acciones de acceso y trabajar offline, e integrar las transacciones de acceso con la plataforma de video a través del software de acceso. Las terminales deben ser instaladas, configurada y puesta en funcionamiento de acuerdo con la marca ofertada.

Certificación del fabricante de software de acceso al oferente como El oferente deberá acreditar certificación vigente como integrador o partner autorizado por el fabricante de los equipos ofertados, que lo habilite para instalación y mantenimiento; se aceptaran certificaciones equivalentes emitidas por el fabricante o su canal de comercialización oficial en el país.</td></tr>
<tr><td>Requisitos específicos</td><td>Características técnicas mínimas:
<table>
<tr><td>Marca</td><td>N/A</td></tr>
<tr><td>Modelo o referencia</td><td>N/A</td></tr>
<tr><td>Capacidad de almacenamiento local</td><td>Debe contar con la capacidad de almacenar mínimo 200.000 identidades, con la capacidad de trabajar fuera de línea del servidor en caso de falla de conexión de red.
Capacidad de almacenar mínimo 450.000 transacciones offline y posterior sincronización con el software de acceso para entrega de datos.</td></tr>
<tr><td>Capacidad de control</td><td>De mínimo 02 terminales de lectura</td></tr>
<tr><td>Alimentación de energía</td><td>12Vdc o POE</td></tr>
<tr><td>Puerto ethernet</td><td>01 puerto de mínimo 10/100Mbps</td></tr>
<tr><td>Entradas</td><td>Mínimo 02 entradas</td></tr>
<tr><td>Capacidad de expansión</td><td>Debe tener la capacidad de soportar mínimo 08 controladores expansores</td></tr>
<tr><td>Direccionamiento</td><td>Debe soportar el direccionamiento de red mediante IPV4, IPV6.</td></tr>
<tr><td>Seguridad</td><td>Debe tener la capacidad de comunicación protegida por TLS ó mínimo AES 128 ó 256 ó FIPS 140-3</td></tr>
<tr><td>Protocolos</td><td>Debe soportar protocolos OSDP y RS485</td></tr>
<tr><td>Funcionalidades mínimas</td><td>Debe soportar múltiples terminales de autenticación de acceso, para barreras de acceso.
Debe tener la capacidad de antirretorno.</td></tr>
<tr><td>Puerto</td><td>Debe contar con puerto microSD o similar</td></tr>
<tr><td>Batería</td><td>Debe contar con batería para el respaldo de memoria y reloj</td></tr>
<tr><td>Salidas</td><td>Debe contar con mínimo 02 salidas de relevo</td></tr>
</table>
</td></tr>
</table>

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Capacidad de control puertas o molinete	Debe tener la capacidad de administrar mínimo 1 puerta o molinete mediante lector biométrico ingreso – lector biométrico salida.
Alarmas	Debe contar con mínimo 01 entradas de alarma Debe contar con mínimo 01 salida de alarma
Temperatura de operación	Debe tener la capacidad de funcionar a mínimo 0° hasta 68°C.
Certificaciones	CE, FCC, RoHS, UL
Húmeda de funcionamiento	Entre 5 a 95% sin condensación
Compatibilidad	Debe ser asegurada con el fabricante de software control de acceso ofertado
Software y accesorios	Debe contar con la última versión de firmware liberada por el fabricante de control de acceso ofertado Debe incluir el cableado de comunicaciones compuesto necesario para la puesta en funcionamiento.
Soporte	El proponente debe adjuntar carta del fabricante que le habilite como canal certificado y con experiencia para la comercialización y el soporte de la solución ofertada en el territorio colombiano
Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
Accesorio o dispositivo	De ser necesario para su perfecto funcionamiento y compatibilidad con los dispositivos del sistema deberá ser suministrado por el proveedor.
Garantía de fabrica	Mínima Dos (02) años

FUENTE DE POTENCIA PARA TARJETAS CONTROLADORAS DE ACCESO

Características técnicas mínimas:

Capacidad	Debe tener capacidad para alimentar y alojar las tarjetas controladoras de acceso
Fuente de alimentación	Debe contar con fuente de alimentación doble, con capacidad de conexión de 110v o 220v
Salida potencia	Debe contar con salida de potencia mínima de 140W a 12v ó 24v con 16 salidas cableadas. Debe contar con salida de potencia mínima de 240W a 12v ó 24v con cargadores de baterías cableados
Gabinete	Debe estar fabricado en acero pintado y contar con cerradura de llave, sensor de apertura de puerta
Compatibilidad	Debe ser compatible para instalar tarjetas controladoras principales IP para control de acceso y tarjetas expansoras de control de acceso.
Placa	Debe contar con placa trasera perforada con separadores y tornillos para la instalación de tarjetas de acceso.
Software y accesorios	Debe incluir los accesorios necesarios para su correcta instalación y funcionamiento. Debe incluir el cableado de comunicaciones necesario para la puesta en funcionamiento.
Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
Accesorio o dispositivo	De ser necesario para su perfecto funcionamiento y compatibilidad con los dispositivos del sistema deberá ser suministrado por el proveedor.
Batería	Debe contar con mínimo 02 baterías para autonomía de mínima de 2 horas en caso de falta de energía.
Garantía de fabricación	Mínima Dos (02) años

Empaque y rotulado	No requiere empaque y/o rotulado especial
Presentación y Unidad de Medida	Unidad

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

ÍTEM 6 SISTEMA DE CONTROL DE ACCESO PARA CARRIL VEHICULAR

<table>
<tr><td>Clasificación del bien o servicio</td><td>
<table>
<tr><th>Clasificación UNSPSC</th><th>Descripción</th></tr>
<tr><td>43211714</td><td>Equipos de Identificación Biométrica</td></tr>
<tr><td>46171619</td><td>Sistemas de seguridad o de control de acceso</td></tr>
<tr><td>72151701</td><td>Servicio de instalación de sistemas de control de acceso</td></tr>
<tr><td>72151704</td><td>Servicio de instalación de sistemas instrumentados de seguridad</td></tr>
</table>
</td></tr>
<tr><td>Nombre Comercial del Bien o Servicio</td><td>Sistema de control de acceso para carril de vehicular</td></tr>
<tr><td>Calidad</td><td>CE, FCC, UL, RoHS.</td></tr>
<tr><td>Generalidades</td><td>Se requiere el suministro e implementación de un sistema avanzado de control de acceso vehicular basado en tecnología de doble factor de autenticación (2FA). El sistema deberá integrar barreras electromecánicas de alto flujo con terminales de lectura que permitan la autenticación mutua mediante reconocimiento facial y tarjetas inteligentes encriptadas. Esta validación se gestionará a través de un protocolo de intercambio de mensajes seguros, garantizando que el acceso se otorgue únicamente tras la verificación positiva de ambas credenciales.</td></tr>
<tr><td>Requisitos generales</td><td>El sistema de control de acceso debe permitir el paso vehicular unidireccional, controlando el ingreso y la salida de vehículos autorizados en el sistema. Debe contar con doble factor de autenticación, que valide el primer factor mediante la lectura de tarjeta MIFARE Plus X4K para autenticación con credencial y el segundo factor mediante el lector de reconocimiento facial para autenticación biométrica.
Certificación del fabricante como empresa certificada en instalación y mantenimiento de los equipos ofertados.

El oferente deberá acreditar certificación vigente como integrador o partner autorizado por el fabricante de los equipos ofertados, que lo habilite para instalación y mantenimiento; se aceptaran certificaciones equivalentes emitidas por el fabricante o su representante oficial en el país.</td></tr>
<tr><td>Requisitos específicos</td><td>
<table>
<tr><th>Componente</th><th>Especificación Técnica</th><th>características</th></tr>
<tr><td>Cámara LPR (Incluye Licencia)</td><td>Con analítica de video</td><td>Cámara en formato tipo bullet IP con IR con capacidad con licencia de reconocimiento de placas integrado en el software de video seguridad existente marca Avigilon para búsqueda rápida.

El software de LPR debe ser de tecnología S top and Go, integrado de manera nativa en el sistema de video seguridad existente.

• Resolución Mínima: 4 Megapíxeles (2592x1520 píxeles)
•Frecuencia mínima: 30 fps (cuadros por segundo) o superior.
•Debe soportar trabajar en temperaturas entre -10° y 65°
•Debe contar con 2 años de garantía por defectos de fábrica.
•Debe contar con certificación NEMA 4x e IP66 ó IP67 e IK10</td></tr>
<tr><td>Cámara de contexto</td><td>Visual</td><td>Debe contar con:

Cámara en formato tipo bullet IP con IR con analíticas de video</td></tr>
</table>
</td></tr>
</table>

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

(Incluye Licencia)		seguridad, integrada el sistema de video seguridad existente • Resolución Mínima: 4 Megapíxeles (2592x1520 píxeles) •Frecuencia mínima: 30 fps (cuadros por segundo) o superior. •Debe permitir visualizar el contexto de la escena de acceso vehicular. •Debe soportar trabajar en temperaturas entre -10° y 65° •Debe contar con 2 años de garantía por defectos de fábrica. •Debe contar con certificación NEMA **4x** e IP66 ó IP67 e IK10

• El software de LPR debe permitir realizar la búsqueda de placas, crear listas de autorizados, listas de no autorizados y generar alerta.

- Interfaz de Gestión: Vinculación de evento de acceso con grabación de video.
  1. Creación de reglas "Placa = Credencial" (la matrícula actúa como el número de tarjeta).
  2. Alertas por vehículos no autorizados en tiempo real.

•Deben contar con IR
•Capacidad de captura reconocimiento, lectura e identificación de placas vehiculares.
•Punto de datos: Debe incluir punto de datos para cada cámara en cat 6A.

Barrera Vehicular

- **Modelo:** Barrera Electromecánica de Alto Tráfico.
- **Velocidad de Apertura:** Entre 1.2s a 3.5s.
- **Longitud del Brazo:** Entre 2 a 3 metros.
- **Ciclo de Trabajo:** 100% (Uso continuo).
- La calidad de la barrera vehicular (talanquera) deben ser de calidad de fabricación equivalente a automatic systems, wolpac o FAAC.
- **Seguridad:** Debe contar con sensor de masa inductivo (loop detector) y fotoceldas de seguridad para evitar cierres sobre el vehículo. Deben ser entregadas instaladas y configuradas en el sitio indicado por la FGN.
- **Controlador:** Debe contar con tarjeta controladora principal IP para control de acceso, integrada de manera nativa al sistema de CCTV existente.
- **Terminal de acceso con doble autenticación facial y tarjeta:** Debe contar con lector facial y tarjeta para validación de acceso, los cuales deben ser de la marca y referencia ofertadas en este anexo técnico.
- **Red:** El contratista deberá suministrar e instalar el cableado UTP Cat6 para cámaras y controladores (PoE+).
- Cableado de comunicaciones: El contratista deberá suministrar el cableado de comunicaciones compuesto especializado para control de acceso (No se aceptará UTP)
- **Energía:** Alimentación 110V/220V para la barrera; respaldo de batería (UPS) para el controlador de acceso.
- **Fuente de potencia para tarjetas controladoras de acceso:** Debe incluir fuente de potencia para las tarjetas controladoras con bateria.
- **Obra Civil:** Base de concreto para barrera y ductería para sensores de piso (loops).
- **Auditoría Total:** Registro de foto de placa + video del conductor + datos del usuario en un solo reporte.
- Reportes de ingreso y salida

El sistema de LPR debe integrarse de manera nativa con el sistema de video seguridad marca Avigilon y almacenar los registros y logs de evento en el servidor NVR existente.
No debe requerirse servidores exclusivos o adicionales para el funcionamiento del sistema LPR.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	El oferente deberá configurar las alertas de detección de placa prohibida y desplegar la alerta en el videowall existente.
Empaque y rotulado	No requiere empaque y/o rotulado especial
Presentación y Unidad de Medida	Unidad
Cantidad	6

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

ÍTEM 7 EQUIPO SERVIDOR PARA MÓDULO DE GESTIÓN DE CONTROL DE ACCESO PARA VISITANTES.

<table>
<tr><td></td><td>
<table>
<tr><th>Clasificación UNSPSC</th><th>Descripción</th></tr>
<tr><td>43211714</td><td>Equipos de Identificación Biométrica</td></tr>
<tr><td>46171619</td><td>Sistemas de seguridad o de control de acceso</td></tr>
<tr><td>72151701</td><td>Servicio de instalación de sistemas de control de acceso</td></tr>
<tr><td>72151704</td><td>Servicio de instalación de sistemas instrumentados de seguridad</td></tr>
</table>
</td></tr>
<tr><td>Nombre Comercial del Bien o Servicio</td><td>Equipo servidor de para módulo de gestión de control de acceso para visitantes.</td></tr>
<tr><td>Calidad</td><td>CE, FCC, RoHS, UL</td></tr>
<tr><td>Generalidades</td><td>Se requiere el suministro con implementación de un equipo servidor de para administración y gestión de control de acceso, con la configuración y puesta en funcionamiento de acuerdo con la marca ofertada.</td></tr>
<tr><td>Requisitos generales</td><td>El equipo servidor de para administración y gestión de control de acceso debe tener la capacidad de procesar la administración del sistema de control de acceso para mínimo terminales de lectura y mínimo 200.000 identidades.</td></tr>
<tr><td>Requisitos específicos</td><td>Características técnicas mínimas:
<table>
<tr><td>Marca</td><td>N/A</td></tr>
<tr><td>Modelo o referencia</td><td>N/A</td></tr>
<tr><td>Hardware</td><td>En este dispositivo se instalará el software de gestión y administración de control de acceso tipo corporativo con integración a sistema de video seguridad</td></tr>
<tr><td rowspan="2">Montaje</td><td>Tipo rack</td></tr>
<tr><td>Máximo 2U de rack de 19”</td></tr>
<tr><td>Procesador</td><td>Un (01) Procesador Intel Xeon E-2330 o Superior</td></tr>
<tr><td>Velocidad de bus</td><td>8 Gt/s</td></tr>
<tr><td>Memoria Ram</td><td>Mínimo 16 GB DDR4 ó DDR5</td></tr>
<tr><td>Almacenamiento</td><td>Mínimo 8Tb</td></tr>
<tr><td>Tipo de discos para almacenamiento</td><td>Discos SATA, SAS o NL-SAS tipo Enterprise para servidores</td></tr>
<tr><td>Capacidad de procesos por minuto</td><td>Debe tener la capacidad de procesar mínimo 48.000 transacciones de acceso por minuto</td></tr>
<tr><td>Conexión ethernet</td><td>Puerto dedicado de administración remota out-of-band compatible con estándares IPMI 2.0 o equivalente</td></tr>
<tr><td>Temperatura de operación</td><td>10°C a 35°C o mejor.</td></tr>
<tr><td>Periféricos</td><td>Ratón y teclado</td></tr>
<tr><td>Lector</td><td>CD-RW / DVD-RW: Interna o externa</td></tr>
<tr><td>Capacidad de procesar puertas</td><td>Debe tener la capacidad de administrar mínimo 380 puertas</td></tr>
<tr><td>Puerto de video</td><td>Mínimo 1x VGA o 1x HDMI</td></tr>
<tr><td>Altura de operación</td><td>El servidor deberá tener la capacidad de funcionar a mínimo 3.000. metros de altura.</td></tr>
<tr><td>Certificaciones</td><td>CE, FCC, RoHS, UL</td></tr>
<tr><td>Húmeda de funcionamiento</td><td>Entre 5 a 80% sin condensación</td></tr>
<tr><td>Fuente de energía</td><td>Con capacidad de trabajar 110 y 220 Vac</td></tr>
<tr><td>Licencias</td><td>Licencias: Sistema operativo preinstalado en</td></tr>
</table>
</td></tr>
</table>

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	fábrica, mínimo Windows o similar.
Software y accesorios	Para configuración e instalación
Máximo consumo de potencia	500W o menor
Soporte	Servicio de soporte y reparaciones en sitio durante el tiempo de garantía de fábrica (Sin costo adicional), incluir certificación expedida por el fabricante.
Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
Accesorio o dispositivo	De ser necesario para su perfecto funcionamiento y compatibilidad con los dispositivos del sistema deberá ser suministrado por el proveedor.
Garantía de fabrica	Mínima Dos (02) años

CARACTERÍSTICAS MÍNIMAS DE MÓDULO DE GESTIÓN DE CONTROL DE ACCESO VISITANTES

El módulo debe permitir realizar gestión de acceso integrado al sistema de control de acceso tipo corporativo ofertado para proporcionar un control eficiente de acceso a nuestras instalaciones.
El módulo debe permitir el enrolamiento de visitantes, captura de registro facial y datos personales para el registro de acceso a las instalaciones de la FGN Nivel central.
El módulo debe permitir la asignación de apertura de puertas de acceso aprobadas por la entidad.
Se requiere que el módulo de acceso de visitantes registre el motivo de la visita, funcionario que autoriza y edificio a visitar.
El módulo de visitantes debe permitir definir la fecha de inicio y la fecha de fin de la autorización de acceso.
Debe incluir el licenciamiento necesario para la instalación, configuración y puesta en funcionamiento

El sistema, debe permitir realizar gestión avanzada de alarmas e identidades de forma fácil y flexible en el sistema para proporcionar un control eficiente de acceso a nuestras instalaciones.
El software debe de funcionar sin interrupciones de forma completa en los diferentes navegadores web de la industria, sin que tengamos limitantes a la hora de realizar gestión, administración o simplemente responder de forma rápida alertas desde cualquier lugar.
El software de control de acceso debe contar con integración con el sistema de video existente en Fiscalía general de la nación, para revisar y verificar las alarmas que se puedan generar en ambos sistemas de forma automática vinculando el evento al momento exacto de video en vivo como grabado para control rápido y respuesta eficiente. Sin costo adicional.
Se requiere que el sistema se pueda configurar bajo en un plano de la Fiscalía general de la nación donde se ubique visualmente la puerta o elemento a monitorear y a su vez se pueda realizar un bloqueo/desbloqueo remoto de puertas incluso en estado de alarma. Sin costo adicional.
Con la integración al sistema de video, la plataforma debe permitir realizar una búsqueda por el nombre de una identidad, los resultados obtenidos sean el momento exacto de video de cuando alguien intento ingresar por una puerta especifica al realizar la marcación correspondiente, de esta manera si se tiene una cámara cerca a la puerta en cuestión, se tenga evidencia fiel de que la persona que ingreso, lo hizo con su propia credencial de acceso. Sin costo adicional.
Se requiere que el sistema opere con Hardware de terceros que este homologado o certificado para trabajar con diferentes marcas de software en la industria, para evitar limitación en implementación y garantizar una estructura de plataforma abierta.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

En caso de falla, el sistema deberá contar con la posibilidad de realiza replicación de bases de datos de identidades del sistema completo en varios dispositivos de forma automática por error en modo de espera activa de los dispositivos para contar con varios niveles de redundancia y resistencia a fallos.
La operación del hardware de campo no debe depender de la operación del servidor de aplicación puesto que, en caso de una falla total del sistema, el sistema de control de acceso debe permanecer operativo.
El sistema de control de acceso debe integrarse al sistema de video seguridad (CCTV) existente en el Bunker Fiscalía general de la nación sin necesidad de licencias adicionales.
Debe proporcionar las facilidades para la verificación de video, combinando el sistema de control de acceso con las cámaras de CCTV ya instaladas en las instalaciones de la Fiscalía general de la nación Nivel central Bunker.
Toda la configuración, el mantenimiento y la interacción con el sistema, se debe obtener sin la interacción con el sistema operativo o la estructura de directorios.
La interfaz de trabajo y configuración de la plataforma de control de acceso deberá ser únicamente vía navegador web, sin la necesidad de requerir una estación de trabajo dedicada. Como mínimo deberá el sistema ser capaz de soportar los siguientes navegadores web: Mozilla Firefox, Google Chrome, Apple Safari.
El uso de servidores de bases de datos separados no será aceptado. “La arquitectura deberá garantizar desempeño y disponibilidad, permitiendo implementaciones centralizadas o distribuidas.”
La plataforma de control de acceso deberá soportar como mínimo, pero no solo estar limitado al siguiente hardware de campo (controladores y subcontroladores) para control de acceso compatibles con al menos 10 diferentes fabricantes, dentro de los cuales deben estar como mínimo la línea de Producto de Mercury Security series 1, 2 y 3, línea de producto de HID Global VertX EVO, línea de producto Salto Systems: Unidad de control CU42E0US y CU4200US.
La plataforma deberá soportar medidas de seguridad para todas las comunicaciones e información de la solución soportando como mínimo SSL 128 bit de encripción o superior.
Debe contar con software de monitoreo y gestión que permite administrar de manera centralizada diversas los diferentes controladores que hagan parte del sistema integrado de control de acceso, además te permitir la interacción con el sistema de video de forma integrada.
La plataforma de control de acceso deberá tener inmersa la funcionalidad de administrar y gestionar multi-sitios.
El software gestión y administración de control de acceso tipo corporativo con integración a sistema de video seguridad debe tener la capacidad de soportar 2048 lectores, y soportar hasta 512 controladores, (50) operadores simultáneos (a través del navegador), sin costo adicional.
Debe ser suministrado el licenciamiento de administración de control de acceso (a perpetuidad) para instalación en para administración y gestión de control de acceso para mínimo 116 lectores.
Debe tener la capacidad de integrarse con las siguientes bases de datos de terceros estándar de la industria, Bidireccional: • Protocolo ligero de acceso a directorios (LDAP/Active Directory). • SQL. • Sistema de gestión de bases de datos relacionales de Oracle. • Valor separado por comas (CSV). • Lenguaje de marcado extensible (XML).
Deber permitir integraciones personalizadas usando Rest API

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	Debe contar con una interfaz de usuario de uso intuitivo que permita ver las siguientes funcionalidades sin limitarse a ellas: • Supervisar eventos, alarmas y estado del hardware en tiempo real. • Verificar identidades en tiempo real. • Buscar eventos históricos y alarmas.
	Debe permitir la configuración de funcionalidades tales como: • Grupos de acceso: Capacidad de crear grupos de terminales de acceso y horarios de modo que las terminales puedan permitir o restringir el acceso a áreas según los horarios. • Registros de Identidad: Proporcionar un sistema con gestión de identidad integrada, permitiendo la importación de datos desde bases de datos soportadas. Cada identidad admite el control de acceso basado en grupos y roles, así como anulaciones individuales. Incluya funcionalidad para personalizar formularios de identidad y token en el software base. Proporcionar registros de identidad capaces de gestión y sincronización entre múltiples sitios. • Roles: Debe tener un método de permiso basado en roles que permite asignar uno o más roles a las identidades para determinar el acceso físico y lógico. • Anti-Passback: Proporcionar un software de control de acceso capaz de designar áreas para requerir una autenticación para ingresar y salir del área antes de que se use para ingresar al área nuevamente. ○ APB de área suave y dura: realiza un seguimiento de cada credencial que ingresa a un área específica y define a qué áreas puede acceder la credencial a continuación. ○ APB basado en puerta: realiza un seguimiento de cada credencial que ingresa y no permite que la misma credencial ingrese dos veces seguida hasta que se alcanza el límite de tiempo de APB. ○ APB cronometrado basado en tokens: realiza un seguimiento de cada puerta a la que ha accedido un distintivo. Después de que la insignia haya accedido a una puerta, debe acceder a una segunda puerta o esperar hasta que se alcance el límite de tiempo de APB antes de poder acceder a la primera puerta nuevamente. ○ APB de área temporizada: APB de área dura basada en tiempo. Cuando expira el límite de tiempo, el área dura APB se convierte en un área blanda APB. ○ Hard Door APB: rastrea cada credencial que ingresa a una puerta y no permite que la misma credencial ingrese dos veces seguida. ○ Soft Door APB: rastrea cada credencial que ingresa a una puerta y genera una transacción de advertencia si la misma credencial se usa en la misma puerta dos veces seguidas. • Macros: Debe proporcionar un sistema capaz de vincular uno o más eventos a macros de modo que un solo evento pueda ejecutar hasta 30 macros. El sistema debe admitir un mínimo de 255 macros por controlador de campo inteligente. • Encryption: Debe proporcionar un sistema de control de acceso que admita los siguientes métodos de cifrado: ○ TLS 1.2: requiere cifrado TLS entre el sistema de control de acceso y el controlador ofertado. ○ Certificados personalizados: requiere un certificado de autoridad certificadora o auto firmado para fortalecer el sistema de control de acceso. Los certificados autenticarán los controladores ofertados en el sistema de control de acceso.
	La plataforma debe contar con un Dashboard • Debe permitir la creación de un tablero para el estado y las acciones en tiempo real de los componentes de hardware en una sola pantalla que también puede filtrar por nombre, estado, dispositivo o grupo. 1. ○ Estado del hardware: Controladores: Comunicación, potencia, sabotaje y batería. Subcontroladores: comunicación, alimentación y manipulación.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	Entradas: inactiva, activa, problema y enmascarada. Salidas: Apagado, encendido y problema. Puertas: Comunicación, sabotaje, batería, desbloqueo, ayuda, enmascarado y forzado. Dispositivos: RAM, programa, base de datos, carga de CPU y estado del puerto. ○ Supervisar: Paneles: estado del dispositivo, estado de seguridad, nombre, modelo, firmware, dirección IP, dirección MAC, tarjetas en uso y última comunicación. Paneles secundarios: estado del dispositivo, nombre, panel, tipo, puerto, dirección y firmware. Entradas: estado del dispositivo, nombre de entrada, subpanel, resistencia EOL y dirección. Salidas: estado del dispositivo, nombre de salida, subcontrolador, programación y dirección. Fuentes de alimentación: nombre de la fuente de alimentación, estado de instalación, estado y registros. Puertas de control de acceso: estado, nombre, panel, estado de la puerta, modo de puerta y estado de anulación. ○ Manipular puertas de control de acceso: Acciones de la puerta: Otorgar, restaurar, desbloquear, bloquear sin acceso, deshabilitar.
	Debe contar con una estación de verificación virtual, esta debe proporcionar una conexión habilitada para navegador web al software de control de acceso para permitir que un usuario confirme visualmente la identidad y la autorización de una persona que intenta ingresar a un área de control.
	Debe permitir coincidencia de servidores, registros de video, de imágenes y seguimientos para auditoría.
	La plataforma debe contar con una Interfaz de mapa: • Deberá proporcionar una interfaz para crear diseños personalizables que incluyan planos de planta, ubicaciones de lectores y botones que pueden desencadenar acciones. ○ Acciones: Indicar la alarma mediante un icono, deshabilitar, desbloquear, bloquear, otorgar, restaurar, enmascarar retenido, desenmascarar retenido y rastrear acciones. ○ Ocupación/reunión: los mapas proporcionarán la ocupación en tiempo real de un área definida. ○ Botones programables: Proporcionar mapas de botones y texto para realizar acciones.
	Soporte remoto: • La plataforma deberá tener la capacidad de soporte remoto para permitir el acceso para soporte técnico y de ingeniería de personal certificado en el software para: ○ Solución de problemas ○ Diagnósticos ○ Carga del Sistema ○ Asistencia con la configuración. Deberá tener la capacidad de obtener datos de registro del log de eventos del software para obtener un mejor soporte de la aplicación.
	Replicación basada en cuadrícula: • La plataforma deberá admitir la arquitectura de replicación basada en cuadrícula automatizada de la estructura de directorios del dispositivo para implementar múltiples dispositivos. ○ La arquitectura de replicación debe ser de igual a igual y no requiere un servidor de base de datos dedicado para permitir la replicación de identidades y datos de configuración en todos los dispositivos. ○ Deberá admitir comunicaciones cifradas entre dispositivos utilizando cifrado SSL. ○ La replicación deberá permitir que los datos LDAP de todos los dispositivos se sincronicen con cada uno de los otros en el sistema, permitiendo que el dispositivo se reconstruya a partir de los datos replicados encontrados en otro dispositivo del sistema.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Funcionalidad Hot Standby: • Debe ser compatible con una arquitectura de hot standby y conmutación por error.   ○ Para cada dispositivo, un dispositivo Hot Standby se deberá configurar para monitorear el estado de su dispositivo asociado principal. En caso de que un dispositivo no funcione, el dispositivo de espera activa debe ser capaz de detectar automáticamente un problema y asumir el control del sistema.
Actualizaciones de software: • La plataforma deberá admitir actualizaciones mediante la descarga desde el sitio web del fabricante o la recepción por correo electrónico de los archivos de actualización. No se deberá requerir interacción física con el dispositivo control de acceso para realizar una actualización exitosa del software del sistema.

Respaldos del sistema:
• Deberá tener la capacidad de respaldar y restaurar la estructura de directorios de LDAP.
  ○ Las copias de seguridad deberán ejecutarse simultáneamente con el resto del sistema y no requerirán que todos los operadores se desconecten del servidor de control de acceso.
  ○ Las copias de seguridad deben incluir datos de transacción y datos de configuración del sistema.
  ○ Las copias de seguridad del dispositivo se pueden cifrar mediante el cifrado AES.
  ○ Copias de seguridad del dispositivo para:
  ▪ Dispositivo de almacenamiento USB
  ▪ Directorio compartido de Windows o carpeta compartida de red
  ▪ Servidores SCP
  ○ Las copias de seguridad se realizarán:
  ▪ Automáticamente en un horario diario predefinido
  ▪ Manualmente a través de la interfaz de usuario.

Deberá soportar como mínimo los siguientes idiomas en su interfaz gráfica a. Ingles b. Español
Plataforma software. a. Debe tener la capacidad de configurar mínimo 60 días feriados b. Debe tener la capacidad de crear mínimo 60 grupos de accesos c. Debe tener la capacidad de generar mínimo 200 zonas de tiempo d. Debe tener la capacidad de gestión de dispositivos con tecnología Wiegand u OSDP e. Debe generar mapas que permiten visualizar las ubicaciones de puntos de control de acceso y el estado f. Debe permitir la configuración de antipassback a todo el sistema
La plataforma deberá tener dentro de sus atributos: La capacidad de control de parqueaderos. Integración con plataformas de video seguridad.
El proponente junto con la oferta deberá adjuntar carta directa de la casa fabricante que lo certifique como empresa integradora certificada, vendedora autorizada y proveedor para el soporte de la marca del sistema de control de acceso ofertado. (No se aceptarán carta de distribuidores mayoristas).
La plataforma de control de acceso debe contar con las funcionalidades desde dispositivos móviles que permita otorgar acceso, bloquear/desbloquear puertas, ver el estado de la puerta en tiempo real, actualizar el estado del acceso o activar un bloqueo en todo el sitio.
La plataforma de control de acceso debe tener la funcionalidad de escenas con un enfoque dinámico para gestionar objetos de seguridad desde una vista personalizable en tiempo real.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	Debe contar con la funcionalidad de escenas y permitir localizar visualmente dónde se encuentran las puertas, cámaras, entradas y salidas en sus instalaciones. Debe permitir utilizar cualquier imagen en archivos BMP, GIF, JPEG, PNG o PDF. Las escenas deben permitir mostrar elementos del panel de control de áreas, incluidas las áreas de reunión.
	La funcionalidad de escenas deberá permitir el bloqueo o desbloqueo de puertas de un sitio.
	La plataforma debe contar con la funcionalidad recopilación de identidades que permitan rastrear en el software de manera interactiva datos en tiempo real, que permite la rápida identificación del personal que falta en caso de una evacuación de emergencia.
	La plataforma de control de acceso debe contar con la funcionalidad de alarmas de manera optimizada, que permita gestionar las alarmas reconocidas, no reconocidas y las programadas.
	Debe ser basado en roles, que definan el acceso físico y lógico de un usuario en función de roles que normalmente están asociados con un grupo de identidades.
	Debe contar con una solución de credenciales integrada que permita diseñar e imprimir credenciales desde el navegador de la plataforma.
	Debe permitir la funcionalidad de reportes pre-existentes así mismo debe permitir personalizar informes para mostrar datos importantes de control de acceso adecuados a la medida para la Fiscalía General de la Nación.
	Debe contar con una herramienta de apoyo a la toma de decisiones intuitiva y basada en la nube, diseñada para mejorar la eficiencia en varios sitios; debe permitir agilizar los informes de incidentes y permitir que los equipos de seguridad sean más ágiles y productivos mediante una interfaz de pantalla única que unifica el video, el control de acceso y una respuesta a incidentes estructurada y personalizada.
	La integración con la plataforma y la herramienta de apoyo a la toma de decisiones basada en la nube, no debe requerir de un gateway cloud externo.
	Debe contar con la funcionalidad o programa de software basado en la nube que unifique las soluciones de seguridad en una herramienta de automatización del flujo de trabajo intuitiva.
	Debe contar con la certificación mínimo dos de las siguientes certificaciones, NDAA, ISO27001.
Empaque y rotulado	No requiere empaque y/o rotulado especial
Presentación y Unidad de Medida	Unidad
Cantidad	01

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada