R3DkODE-39

R4D1C4D0

SONDEO DE MERCADO

La Agencia Nacional de Hidrocarburos –ANH está adelantando el presente sondeo de mercado, con el fin de realizar el análisis económico y financiero que soportarán la determinación del presupuesto oficial de un posible proceso de selección contractual, si su Empresa se encuentra interesada en participar le agradecemos remitir la información solicitada, bajo los parámetros establecidos a continuación.

NOTA: *La Agencia Nacional de Hidrocarburos – ANH, aclara que ni el envío de esta comunicación ni la respuesta a la misma generan compromiso u obligación de contratar, habida cuenta que no se está formulando invitación para participar en un concurso o proceso selectivo, sino, se reitera, se está realizando un sondeo de mercado del que eventualmente se puede derivar un proceso de selección para la elaboración de un contrato que permita ejecutar el proyecto*

DESCRIPCIÓN DE LA NECESIDAD:	La Agencia Nacional de Hidrocarburos, necesita adquirir un sistema de integrado de seguridad electrónico conformado por un CCTV y Control de Acceso para la oficina principal de la ANH ubicado en la Avenida Calle 26 No. 59-65 en los pisos 1, 2, 3 y 4. El sistema debe garantizar el control de acceso de funcionarios, contratistas y visitantes, así como los la vigilancia a través de sistema de cámaras que permita la tele vigilancia eficiente y confiable de todos los recintos sensibles y estratégicos de la ANH.
OBJETO A CONTRATAR:	"Adquisición del sistema integrado de seguridad electrónico (CCTV-control de acceso)"
IDENTIFICACION DEL CONTRATO A CELEBRAR:	Contrato de compraventa
CÓDIGO UNSPSC (The United Nations Standard Products and Services Code® - UNSPSC, Código Estándar de Productos y Servicios de Naciones Unidas), correspondiente al bien, obra o servicios a contratar:	Con arreglo a los artículos 2.2.1.1.1.5.1. al 2.2.1.1.1.5.7. del Decreto Reglamentario 1082 de 2015, los Proponentes Individuales deben encontrarse inscritos, clasificados y calificados en el Registro Único de Proponentes – RUP de la Cámara de Comercio de su domicilio principal, en alguno (s) o en todos de los siguientes Códigos Estándar de Productos y Servicios de Naciones Unidas (UNSPSC):

<table>
<tr><td></td><td>
<table>
<tr><th>SEGMENTO</th><th>FAMILIA</th><th>CLASE</th><th>PRODUCTO</th><th>NOMBRE</th></tr>
<tr><td>46</td><td>17</td><td>16</td><td>19</td><td>Sistema de Seguridad o de control de acceso</td></tr>
<tr><td>46</td><td>17</td><td>16</td><td>22</td><td>Sistema de televisión de circuito cerrado CCTV</td></tr>
<tr><td>72</td><td>15</td><td>17</td><td>04</td><td>Servicio de instalación y mantenimiento de sistemas instrumentados de seguridad</td></tr>
</table>

En el caso de propuestas presentadas por consorcios, uniones temporales o promesas de sociedad futura, <u>cada uno de los integrantes</u> debe encontrarse inscrito, clasificado y calificado en por lo menos uno de los Códigos anteriormente establecidos.</td></tr>
<tr><td>ASPECTOS TÉCNICOS:</td><td>Ver Anexo 1 (Especificaciones técnicas de Sondeo)</td></tr>
<tr><td>LUGAR DE EJECUCIÓN:</td><td>El lugar de ejecución del proyecto y la prestación del servicio de mantenimiento preventivo y correctivo es la Avenida Calle 26 No 59-65 Piso 1, 2, 3 y 4 en la Ciudad de Bogotá.</td></tr>
<tr><td>PROPUESTA ECONÓMICA:</td><td>Ver Anexo 2(Propuesta económica) NO MODIFICAR POR FAVOR</td></tr>
</table>

ENTREGA DE INFORMACIÓN DEL SONDEO DE MERCADO: Las firmas invitadas deberán entregar la información solicitada en el presente sondeo de mercado al correo electrónico: **jorge.castillo@anh.gov.co,** antes del día **08 de agosto de 2016.**

ANEXO 1 - ESPECIFICACIONES TÉCNICAS

REQUERIMIENTOS FUNCIONALES Y TÉCNICOS MÍNIMOS

A continuación se describe las características técnicas y funcionales que deben ser cumplidos para el sistema de seguridad electrónica a implementar en la ANH.

SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

Descripción del Sistema

Se requiere un Sistema de Circuito Cerrado de Televisión (CCTV) de última generación, con tecnología de video digital (Video IP), para permitir la tele vigilancia eficiente y confiable de todos los recintos sensibles y estratégicos de las dependencias del edificio.

El control del sistema de CCTV debe estar basado en una plataforma de administración de video digital (Video IP), conformada por un servidor de administración de base de datos, servidores de almacenamiento de video IP, estaciones de trabajo de clientes, pantallas de visualización, y cualquier otro elemento que resulte necesario.

El Sistema de Circuito Cerrado de Televisión tendrá una arquitectura Cliente-Servidor o a través de un acceso Web, basado en una red modular utilizando sistemas operativos estándar, redes y protocolos. La red será del tipo Ethernet a desarrollar en sinergia con el sistema de cableado estructurado (corrientes débiles) que se considerará con el proyecto y debe convivir con el sistema de cableado existente.

Asimismo, se requiere la adecuación de la sala de control, donde se centralice la visualización y control del 100% de las cámaras en tiempo real y con alarmas que tempranas que permita a los operadores de seguridad (Guardas de Seguridad) identificar situaciones diferentes a la operación normal. El sistema debe poder permitir:

- Identificar un posible intruso.
- Verificar al instante la causa de una alarma generada automáticamente.

De acuerdo a los requerimientos de equipamientos de seguridad que se han establecido para la Entidad, las cámaras de CCTV deben ser ubicadas de manera tal que se cubra la totalidad de pasillos, puertas externas e internas, así como los recintos definidos como criticidad alta por la ANH.

El sistema de CCTV debe ser integrado con el sistema de Control de Accesos, que debería considerar una cámara de CCTV asociada a cada puerta controlada con

lectores de proximidad, las cuales estarán grabando permanentemente la actividad en cada puerta.

Todas las señales de video deben ser controladas en el cuarto de monitoreo, donde los Operadores podrán efectuar las labores de vigilancia en vivo o de análisis de las imágenes grabadas.

Cada cámara de acuerdo a su tipo y zona a vigilar, debe presentar una imagen al operador, el cual la utilizará de acuerdo a sus posibilidades o requerimiento. Para esto el operador debe tener a su disposición las siguientes herramientas:

- Mecanismos de control de movimientos de cámara.
- Control de acercamiento (Zoom).
- Controladores de señal (Switch).
- Almacenamiento digital.

Para proporcionar a los Operadores del sistema de tele vigilancia de un adecuado control o manejo de las cámaras hacia los monitores de vídeo, el software de aplicación debe incluir la función de Matriz Virtual de Vídeo que permite direccionar a través de software las entradas (señal de las cámaras de vídeo) hacia las salidas (serie de monitores de vídeo).

Con la función Matriz de Vídeo se debe programar:

- Las secuencias de cámaras en un monitor.
- Las cámaras que serán mostradas en cada monitor existente en el sistema.
- Programar las secuencias de movimiento para las cámaras con movimiento.
- Seleccionar una cámara a un evento de alarma.

Tecnología de cámaras

Todas las cámaras de vídeo deberán incorporar la tecnología IP/POE, de tal manera de aprovechar la red Ethernet propia del Sistema de Seguridad para realizar la transmisión de las imágenes y la alimentación eléctrica de las mismas mediante el mismo cable de red.

Esta combinación permite la digitalización y compresión del vídeo para luego ser transmitida a través de la red Ethernet de Seguridad en la cual se deben considerar Switch distribuidos para conducir todas las señales de video hasta los servidores de cámaras del sistema.

Las cámaras de vídeo IP deben tener las tienen las siguientes características:

- Posibilidad de utilizar cámaras de vídeo de alta resolución (Megapíxel).
- Calidad de imagen constante.
- Redundancia en el control y almacenamiento de las señales de video.
- Permitir a los usuarios, que tengan las autorizaciones correspondientes, realizar gestión sobre el vídeo, guardarlo y por supuesto visualizarlo, en forma local o remota a través de la red disponible.
- Alimentación a través de la red (Switch POE).

Arquitectura del Sistema de CCTV

El Sistema de Circuito Cerrado de Televisión deber estar integrado al Sistema de Control de Acceso. Los Operadores podrán acceder en forma integral a todas las aplicaciones de control y seguridad desde una misma Estación de Cliente, sin necesidad de cerrar una aplicación para abrir otra.

La arquitectura general del sistema centralizado soportará servidores distribuidos de manera de permitir a sistemas múltiples e independientes, comunicarse entre sí para la transferencia de datos de manera de proveer una fácil y adecuada administración del sistema de seguridad y evitar la duplicidad de ingeniería.

El sistema centralizado debe permitir la distribución de ciertas funciones del sistema, tales como la supervisión, control e interface gráfica de usuario, a través de toda la red de manera de permitir un máximo de flexibilidad y rendimiento.

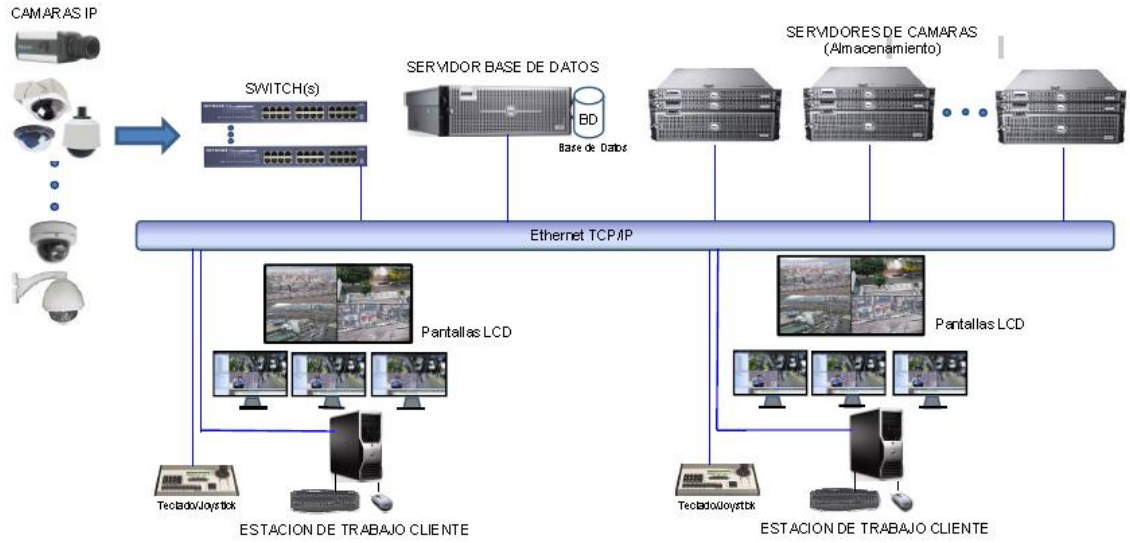
La arquitectura del sistema deberá incluir el soporte de varias redes de área local (LAN y WAN) utilizando hardware y software estándar para enlazar nodos en un solo sistema integrado. El protocolo de red a utilizar deberá ser TCP/IP estándar.

El Sistema de Circuito Cerrado de Televisión podrá ser operado y supervisado desde el Sistema Centralizado a través de cualquiera de sus Estaciones de Trabajo en una sesión de Operador con los permisos y autorizaciones correspondientes.

En particular, el sistema de administración digital de circuito cerrado de televisión, estará conformado por los siguientes elementos:

- Software de Aplicación.
- Servidor de Base de Datos.
- Servidores de Cámaras (almacenamiento).
- Estaciones de Clientes (Operadores).
- Teclados de Operación.
- Cámaras IP/POE.
- Infraestructura de red.

En el siguiente diagrama se muestra la arquitectura del equipamiento en la Sala de Control.



Una red LAN Ethernet exclusiva para los sistemas de seguridad, será implementada por el instalador de los sistemas de seguridad, por lo cual se debe contemplar si es necesario la instalación de backbone de fibra óptica para interconectar los Switch instalados en los cuartos de comunicación, interconectando además con el cuarto de monitoreo y el Centro de Computo Principal CCP.

Todos los Switch que reciben las señales de las cámaras de CCTV estarán conectados a los backbone de fibra óptica, que mediante dos fibras se conectarán a la red LAN Ethernet exclusiva del Sistema de Seguridad. De esta manera todas las señales digitales de las cámaras de vídeo, a través de Cableado Estructurado, llegarán al CCP. Los Switch deberán tener las características de capacidad, velocidad y administración, para asegurar la adecuada comunicación de todas las cámaras.

Donde las distancias a las cámaras de CCTV lo permitan los Switch deberán tener la capacidad POE para alimentación de las cámaras.

Servidores de Base de Datos.

El Servidor de la Base de Datos contendrá la base de datos de todas las cámaras conectadas a la red del sistema y su configuración.

El Servidor de Base de Datos debe permitir:

- Administrar la Base de Datos, incluyendo:
  - Configuración del Sistema
  - Configuración de parámetros de las cámaras
  - Configuración de parámetros de los codificadores de video
  - Configuración de parámetros de grabación
  - Horarios de grabación y supervisión
  - Perfiles de Operadores
  - Configuración de visualización de pantallas de los Operadores
  - Configuración de Monitoreo de Alarmas
  - Configuración de Teclados
  - Configuración de Video Analítico
  - Detección de Movimiento
  - Seguimiento de Objetos
  - Clasificación de Objetos
  - Video Analítico inteligente
  - Detección de Intrusión
- Administración de comunicaciones entre la Estación de Trabajo del Operador y los Servidores de Cámara.
- Permitir acciones de grabación en eventos de alarmas.
- Soportar conexiones múltiples a Servidores de Sistemas de Alarmas o de Control, los cuales podrán recibir video en vivo o grabado desde el sistema de CCTV.
- Reportar situaciones de fallas de cámaras o grabación.
- Proveer registros del estado del sistema y de acciones del operador.
- Utilizar Microsoft SQL Server 2008 como motor de Base de Datos.

El Servidor de Base de Datos debe permitir ser utilizado en una configuración redundante, usando dos Servidores de Base de Datos separados (siendo ejecutados en computadores separados. El Servidor redundante deberá ser sincronizado continuamente con el servidor maestro de manera de asegurar que está siempre actualizado y siempre listo para “fail-over” cuando sea requerido. Debe ser posible remover uno de los dos servidores para efectos de mantención sin interrumpir la operación del sistema, y en la reposición, se deberá re-sincronizar también sin interrupción.

El Servidor de Base de Datos deberá cumplir al menos las siguientes especificaciones de hardware, sistema operativo y software:

- Intel Xeon Q9400 Quad Core o equivalente AMD.
- 4Gb RAM.
- Disco Duro suficiente para requerimientos de la aplicación.
- Tarjeta de Red (NIC) 1000 Mbps.
- Tarjeta Gráfica con 32-bit color y 1Gb video RAM.

- Windows 2008 Server Edition de 64-bit o Windows 7 Professional Edition de 64-bit.
- Microsoft SQL Server 2008.
- Microsoft Internet Explorer 6.0 con Service Pack 1 or superior

Plataformas de hardware propietarias no serán aceptables y los Servidores de Base de Datos deben considerar la siguiente tolerancia a fallas del sistema:

- Soporte RAID 0+1, 1, 3 o 5 para el Sistema Operativo
- Soporte RAID 0+1 o 1 para el Base de Datos (SQL Server 2008)

Servidores de Cámaras (Almacenamiento)

Con el almacenamiento digital se podrán grabar todas las cámaras con diferentes parámetros de velocidad (cuadros por segundo) y resolución, y además reproducir las imágenes en la fecha y hora seleccionada.

El almacenamiento de las imágenes de video digitalizadas y comprimidas se deberá realizar en servidores de almacenamiento, también denominados “Servidores de Cámaras”, los cuales deben tener las características de hardware y software para garantizar el almacenamiento durante sesenta (60) días, en lo que se refiere a velocidad de proceso y capacidad de disco duro.

Los servidores de almacenamiento o servidores de cámaras permitirán grabar señales de video de hasta 30 cuadros por segundo y alta resolución (4CIF). También se permitirá grabar señales de video del tipo mega-pixel, audio y datos. Para determinar la capacidad de disco duro en cada servidor, se deberá utilizar como promedio 15 cuadros por segundo, resolución 2CIF y grabación continua con un promedio de 30% de actividad en la imagen.

El sistema deberá soportar múltiples Servidores de Cámaras (almacenamiento) y tendrán además las siguientes características y funciones:

- Fuentes de alimentación y unidades de disco duro que se instalan sin necesidad de apagar y encender el equipo.
- Tolerancia de fallas mediante el uso de almacenamiento RAID 5 y fuentes de alimentación y ventiladores redundantes.
- Registro de errores, monitoreo y diagnósticos del sistema.
- Control y administración remotas completas a través de la red.
- Administrar las señales de video de las cámaras y codificadores.
- Transmitir video en vivo y grabado a las Estaciones de Trabajo de Operador.
- Transmitir video a los eventuales Servidores de Video Analítico.

- Recibir comandos de control de las Estaciones de Operador y de Teclados y enviar esos comandos a las cámaras.
- Almacenar video y audio en los discos duros.
- Proveer funciones de video analítico, incluyendo detección de movimiento y seguimiento de objetos.
- Exportar grabaciones en formatos universales, tales como Windows Media.
- Permitir la supervisión de alteración de cámaras, tales como, cambio de ángulo de visión, imagen borrosa y cámara obstruida.
- Recibir eventos de cámaras IP o codificadores de video y reaccionar de acuerdo a configuraciones pre-establecidas, tales como: comienzo de grabación y envío de alarmas.
- Transmitir comandos de salida a los puertos de las cámaras IP.

Los Servidores de Cámaras deberán cumplir como mínimo las siguientes características de hardware y sistema operativo:

- Intel Xeon Q9400 Quad Core o equivalente AMD.
- 4Gb RAM + requerimientos de grabación de pre-eventos
- Disco Duro suficiente para requerimientos de grabación
- Dos Tarjetas de Red (NIC) de:
  - 100/1000 Mbps para transmisión de video a las Estaciones de Operador
  - 100/1000 Mbps para transmisión de video desde cámaras IP.
- Tarjeta Gráfica con 32-bit color y 1Gb video RAM si el Servidor de Cámara también es usado como Estación de Cliente.
- Windows 2008 Server Edition de 64-bit o Windows 7 Professional Edition de 64-bit.
- Microsoft Internet Explorer 6.0 con Service Pack 1 or superior

Multiprocesamiento y Tolerancia a Fallas

El Servidor de Base de datos y Servidor de Cámaras (cuando sea requerido) deberán permitir la operación en computadores de procesadores unitarios y múltiples. Cuando se utilice un sistema multiprocesador, el software de aplicación deberá ser capaz de optimizar el uso de la configuración.

Una falla en cualquiera de los Servidores de Base de datos o Servidores de Cámara, no deberá dejar inoperativo al sistema de CCTV. Como peor caso, solo las cámaras controladas por el Servidor de Cámaras en falla quedarán temporalmente inhabilitadas hasta que sean reubicadas en otro Servidor de Cámaras utilizando el software de aplicación, No se deberá requerir ningún cambio físico al hardware, cableado o conexiones.

Estaciones de Operador

El control del sistema y la visualización de las señales de video se deben permitir a través de uno o más Estaciones de Trabajo de Operador. Estás máquinas deberán ser conectadas vía la red TCP/IP al Sistema de Control de Acceso/CCTV y podrán visualizar video en vivo y grabado desde las Servidores de Cámaras a través de accesos autorizados por claves de seguridad.

El Sistema además permitirá una interface de cliente de Microsoft Internet Explorer para la visualización y grabación de video, búsqueda de video, reproducción de video, configuración del sistema y administración del sistema.

El Operador debe tener la capacidad de desplegar hasta 16 señales de video en variadas configuraciones y con presentaciones en formato estándar 4:3 y 16:9, sin distorsión del video y utilizando toda el área de la pantalla.

Las Estaciones de Operador deberán cumplir al menos las siguientes especificaciones de hardware, sistema operativo y software para permitir la integración de video:

- Intel Xeon Q9400 Quad Core o equivalente AMD.
- 4Gb RAM.
- Disco Duro suficiente para requerimientos de la aplicación.
- Tarjeta de Red (NIC) 1000 Mbps.
- Tarjeta Gráfica con 32-bit color y 1Gb video RAM.
- Windows 2008 Server Edition de 64-bit o Windows 7 Professional Edition de 64-bit.
- Microsoft SQL Server 2008.
- Microsoft Internet Explorer 6.0 con Service Pack 1 or superior.
- Tres (3) Monitores LED de 40", 1080p (1920x1080), DVI, HDM VGA, Composite, Widescreen, Built-in Speaker (10W), V

Las Estaciones de Operador deben permitir y operar la instalación de la interface cliente del sistema de CCTV dentro de la misma interface cliente utilizada por el Sistema de Control de Accesos (Seguridad).

Teclados de Operador

El sistema de CCTV debe considerar uno o más teclados de CCTV de tipo profesional, con Joystick, el cual deberá estar integrado al sistema a través de una conexión a la red Ethernet de seguridad.

El Teclado de Operador deberá permitir el control y visualización de las señales de video sin la necesidad de una Estación de Operador y deberá permitir las siguientes funciones:

- Acceder al sistema (Log on)
- Seleccionar cámaras y monitores
- Seleccionar múltiples cámaras en monitores
- Seleccionar y controlar cámaras mediante un Joystick
- Iniciar y detener grabaciones
- Salir del sistema (Log Off)

Los Teclados de Operador podrán ser configurados desde el software de aplicación.

Cámaras y Codificadores de Video

El Sistema de Administración y Grabación de Video deberá permitir un crecimiento.

Las cámaras IP podrán ser utilizadas en el sistema digital de video serán de marcas reconocidas, con certificaciones de calidad reconocibles, experiencias de instalaciones en Colombia y con empresas integradoras certificadas establecidas en Colombia.

Todas estas marcas deberán ser compatibles en la conectividad, protocolo y funciones del software de aplicación del sistema de administración y grabación de video, para obtener el 100% de operatividad con el software de integración de control centralizado con CCTV y Control de Accesos.

Considerando para las cámaras IP, se debería considerar técnicamente al menos:

- Deben contar Streams de video tipo “On Demand” es decir que, no enviarán a la red todo lo que capturen, sino solamente el video que le están solicitando. Así como la posibilidad de configurar QoS (Calidad de Servicio) mediante web browser o por consola de comandos (CLI).

- Contará con el sistema Port Authentication 802.1EAP que permite a las cámaras autentificarse ellas mismas a una red de datos, tal como un usuario lo hace en un PC. Esto permite al administrador de red, asegurar sus puertos en uso, de modo que solo los dispositivos autorizados podrán utilizarlas.

- Compatibilidad con Object Video: Las cámaras que lo requieran deberán contar con Inteligencia o Video Analítico el que deberá ser compatible con OV ready, además esta característica permitirá ser configurada ya sea

desde la plataforma de administración como a través del web browser de la cámara. Conforme a este punto se solicitará que este tipo de cámaras cuente con analítica de sabotaje, el que detectará automáticamente al operador si la cámara está siendo manipulada, tapada u obstaculizada por algún agente externo que impida ver la escena con normalidad.

- Exposure Profiles: Los perfiles de exposición permiten cambiar la gama de colores en función de la exposición de la escena, no confundir con brillo, saturación y contraste.

- Low Light Technology: incorporará tecnología de baja iluminación que permite una excelente calidad de imagen en condiciones mínimas de luz, sin la necesidad del uso adicional de elementos como luces IR.

- Auto Back Focus: Elemento indispensable en las cámaras Megapíxeles que permite un Foco Trasero Automático, el cual mantiene una escena siempre enfocada, independiente de los cambios repentinos de iluminación, movimiento o temperatura que pudiesen existir en un sitio o en una escena, de este modo se consigue una imagen perfecta en todo momento. El ABF podrá ejecutarse directamente desde la cámara a través de un botón, o por medio del web browser.

Cámara Fija Interior tipo Mini-Domo

Las cámaras que están ubicadas en el interior de los recintos del edificio serán del tipo Mini-Domo con montaje en cielo. Estas cámaras serán formato color NTSC, día noche verdadero, alta resolución y lente varifocal de manera de ajustar el ángulo de visión de acuerdo a las necesidades de cara posición. Las características deberán ser las siguientes:

CARACTERÍSTICA	DESCRIPCIÓN
Dispositivo de Imagen	1/3 " CMOS
Scan	Progresivo
Auto Back Focus (ABF)	Si
Rango Dinámico Amplio (WDR)	60dB
Iluminacion	Color 0,12Lux - BW 0,03Lux
Video Compresión	MPEG4-CVBR / MJPEG / H.264 Hi Pro
Resolución	3,2 MPx (1280x1024) 30fps
Analítica	On borrad - Sabotaje
Almacenamiento Interno	SD Card

QoS	Si
Seguridad	802.1EAP
PoE	802.3af

Cada cámara deberá considerar un lente Megapíxel del tipo varifocal. La cantidad de mm a definir en la escena o en los planos, conforme a referencia requerida.

Cantidad de Cámaras Fija Interior tipo Mini-Domo

Se requiere instalar un total de treinta y ocho (38) cámaras tipo de Domo en la instalación de la ANH de acuerdo a las necesidades establecidas por la Agencia.

Cámara 360°

Se consideraría una cámara del tipo “fisheye” de bajo perfil con las siguientes características:

- Compact diameter 108mm (4 ¼")
- 5MPx 1/2.5 CMOS sensor
- H.264 / MJPEG Multistream
- 0.2 lux
- IEEE802.3af Class 2 POE or 12VDC
- Ceiling / Wall / Table mount
- Compatible with Oncam Grandeye 3D dewarping software
- Client-side dewarping on Pelco Digital Sentry and other compatible VMS platforms
- ONVIF Profile S Compliant

Cantidad de Cámaras 360°

Se requiere instalar un total de veinticuatro (24) cámaras tipo de 360°en las instalaciones de la ANH de acuerdo a las necesidades establecidas por la Agencia.

Red Ethernet y Cableado de Red.

En forma exclusiva para el sistema de seguridad (video, control de acceso y seguridad) se deberá implementar una red de área local (LAN) Ethernet para las comunicaciones entre los elementos del sistema. Todas las interfaces a la red LAN deberán ser como mínimo Ethernet 100BaseTX. La red LAN podrá considerar adicionalmente otras tecnologías dentro del back bone para permitir mayor velocidad o distancia, entre las cuales se aceptarán las siguientes:

- FDDI
- 100BaseFX

- 1000BaseSx o 1000BaseLX Gigabit
- ATM (Asynchronous Transfer Mode)

La red LAN utilizará Fibra Optica multi-modo para todos los backbone verticales y horizontales y cable UTP (par trenzado no blindado) mínimo Categoría 6 para las conexiones entre las cámaras o codificadores de video y los Switch en el backbone.

Cada Switch conectado a la red deberá soportar:

- Protocolo SNMP (Simple Network Management Protocol)
- IEEE 802.1D Capacidad de Puente y detección de loop
- IEEE 802.1Q tagged VLANs
- IEEE 802.1p traffic prioritization for multiple Quality of Service levels
- IEEE 802.1w rapid spanning tree with fast link support
- IEEE 802.3ad link aggregation support
- IGMP snooping for IP Multicast support
- Multicast network traffic
- Non-blocking configuration capable of simultaneous wire-speed switching across all ports.

La red LAN deberá ser lógica y físicamente independiente y separada de cualquier otra red LAN da la ANH. La interconexión con otras redes LAN o WAN podrá ser a través de los siguientes medios:

Todas las cámaras IP o codificadores de video deberán poseer una única interface de red para ser utilizada para comunicaciones de video.

Canalizaciones y Alambrado

El proyecto de Corrientes Débiles considera la instalación de bandejas de corrientes débiles a través de todos los recintos, pasillos y áreas comunes. El instalador del Sistema de CCTV deberá canalizar desde el punto de las cámaras de CCTV hasta estas bandejas disponibles, lo cual se podrá ejecutar ducto EMT de 1”

El Cableado desde las Cámaras tipo IP de CCTV hasta los Switch se deberá ejecutar en cable de red mínimo de Categoría 6.

Software de Aplicación

Video en vivo

El video en vivo de las cámaras será configurado y visualizado a través de una serie de display. Esta configuración deberá permitir lo siguiente:

- Visualización de una cámara.
- Visualización de múltiples cámaras hasta 16 cámaras simultáneas, cada una a 30 cuadros por segundo.
- Visualización de secuencias de cámaras.
- Opción de visualización en formato 4:3 y 16:9 sin distorsión en toda la pantalla.
- Modificación de configuración de las cámaras.
- Modificación de configuración de grabación de las cámaras.
- Detección de Pérdida de Video. Indicación en pantalla y registro.
- Alteración de Cámaras. Cambio de ángulo, imagen borrosa y obstrucción, configurable por cámara.
- Agregar y eliminar cámaras.
- Creación de horarios de grabación, video analítico y supervisión.
- Modificación de parámetros de video analítico.
- Modificación de Parámetros de entrada, salida y tamper de cámaras.
- Manejo de audio bidireccional con cámaras con audio.

Los operadores podrán seleccionar cámaras de un listado en configuración de “árbol” con todas las cámaras permitidas para ese Operador.

El sistema debe permitit la utilización de múltiples tipos de pantallas:

- Monitor de visualización de video.
- Monitor de Control de Accesos.
- Monitor de Alarmas.
- Combinación de Monitor de video y alarmas.

En cualquiera de estos casos, los monitores adicionales podrán ser conectados a una Estación de Operador con PC multi monitor o a otro PC. No se aceptarán software de aplicación que no permita esta funcionalidad de tipos de monitores.

Cámara Individual

En la visualización de cámaras individuales, el software debe permitir:

- Visualizar el video de la cámara seleccionada.
- Ejecutar PTZ utilizando un Joystick conectado a la Estación del Operador.

- Ejecutar PTZ utilizando recursos de Windows (mouse, touch screen).
- Grabación manual de video.
- Grabación manual de imágenes instantáneas (fotos).
- Indicación de habilitación de la detección de movimiento.
- Visualizar nombre de cámaras en la pantalla.

Cámaras Múltiples

El software de aplicación deberá permitir visualización de múltiples cámaras, consistiendo en hasta 16 cámaras simultáneas en una pantalla, en las configuraciones siguientes:

Formato estándar 4:3

- Una cámara y secuencias de cámaras (con configuración de tiempo).
- 2 x 2 cámaras.
- 3 x 3 cámaras.
- 4 x 4 cámaras.
- 1 + 5 cámaras.
- 2 + 8 cámaras.
- 1 + 12 cámaras.

Formato ancho 16:9

- Una cámara y secuencias de cámaras (con configuración de tiempo).
- 2 x 3 cámaras.
- 3 x 4 cámaras.
- 1 + 3 cámaras.
- 2 + 4 cámaras.
- 1 + 8 cámaras.

Se podrá visualizar el nombre de las cámaras para cada cámara y preset.

Configuración de Cámaras

Los Operadores, dependiendo de sus niveles de autorización de accesos al sistema, podrán configurar los parámetros de las cámaras IP o codificadores de video:

- Información de cámaras (Nombre, número, ubicación y descripción).
- Conexión de la cámara.
  - Tipo de cámara.
  - Resolución
    - 160x120
    - QCIF (PAL 192x144, NTSC 176x112)
    - 240x180

  - 320x240
  - CIF (PAL 384x288, NTSC 352x240)
  - 480x360
  - 640x480
  - 2CIF (PAL 768x288, NTSC 704x240)
  - 4CIF (PAL 768x576, NTSC 704x480)
  - Half-D1 (PAL 720x288, NTSC 720x240)
  - D1 (PAL 720x576, NTSC 720x480)
  - 800x600
  - 1024x768
  - Megapixel (1600x1200, 1280x1024, 1280x960 and 1280x720)
- Formato de compresión (Motion JPEG, MPEG-1, MPEG-2, MPEG-4 y H.264).
- Velocidad (hasta 30 cuadros por Segundo).
- Nivel de compresión (hasta 5 niveles de compresión).
- Dirección IP.
- Número de entrada en codificadores de entrada múltiple.
- Limitación de ancho de banda.
  - Sin restricción
  - 2.0Mb/s
  - 1.5Mb/s
  - 1.0Mb/s
  - 512kb/s
  - 256bk/s
  - 128kb/s
  - 64kb/s
- Transmisión de video unicast o multicast.
- Selección de video, audio unidireccional y audio bi-direccional.

- Seguridad. (Autorización de Usuarios, prioridad d control).
- Creación y Eliminación de Cámaras, dependiendo de nivel de autorización.

Grabación

La grabación de video es almacenada en los Servidores de Cámaras. La estación de Operador debe tener la capacidad de buscar y ubicar grabaciones de video relevantes para luego reproducirlas en la Estación de Operador.

Los siguientes métodos de grabación deben ser permitidos:

- Activación por el operador.
- Activación por eventos.
- Activación por señal de entrada/salida de cámaras IP o codificadores de video.
- Activación por Calendario/Horario.
- Grabación continúa.

- Por Video Analítico (Detección de Movimiento).
- Grabación de Fotos.

Dependiendo del tipo de activación de la grabación, se deben considerar las siguientes configuraciones:

- Duración de grabación pre-evento.
- Duración de Grabación Post-evento.
- Velocidad de grabación.
- Periodo de almacenamiento.
- Archivo de imágenes.
- Borrado de grabaciones.

Reproducción de gra*b*aciones

Los videos grabados deberán estar disponibles para todos los usuarios que tengan el nivel de seguridad suficiente. Cada operador solo podrá reproducir video para los cuales está autorizado.

El software de aplicación deberá disponer las siguientes funciones y control:

- Un panel de navegación para seleccionar cámaras.
- Un control de calendario para seleccionar la fecha del video a reproducir.
- Listado de grabaciones para una cámara para la fecha seleccionada.
- Controles de reproducción de video.
- Información relacionada con la grabación seleccionada.
- Control de almacenamiento del video seleccionado.

Búsqueda de grabaciones

El software de aplicación deberá permitir la búsqueda simple para todas las grabaciones de video de una cámara, donde el Operador podrá seleccionar la fecha y período de tiempo de la grabación que requiere.

El Operador podrá realizar una búsqueda de una combinación de cámaras, en una selección de fecha y período de grabación.

Los criterios mínimos de búsqueda deberán ser los siguientes:

- Tipo de grabación (manual, evento, video analítico, supervisión, entrada/salidas).
- Alarma o evento.

- Área o sector.
- Nombre o número de la cámara.
- Descripción de un evento.
- Nombre del Operador.
- Comentarios incluidos en las grabaciones.

Auditoria de Operadores y Sistema

Todas las acciones de los usuarios en las estaciones de Operadores sean grabadas y registradas para posterior auditoría.

Las acciones de usuarios que deben ser registradas como mínimo son las siguientes:

- Intervenciones tales como grabación manual y cambios de configuración.
- Cámaras visualizadas.
- Grabaciones reproducidas.
- Grabaciones exportadas.

Este registro debe también contener la historia del estado de los componentes del sistema de CCTV. Deberá listar el estado de todas las cámaras, codificadores de video, servidores y cualquier otro componente del sistema incluyendo cuando son deshabilitados o en situación de falla.

El registro de acciones de usuario y sistema deberán estar disponibles y automáticamente incluidos en cualquier exportación de video.

Firma Digital de Grabaciones y Registro de Auditoría

Todos las grabaciones y registros de auditoría que sean exportados deberán tener una firma digital de manera de probar autenticación (origen de la grabación y registro) e integridad (grabación y registro sin alteraciones).

El software de aplicación deberá proporcionar un certificado digital base por las grabaciones y registros de auditoria exportados. Este certificado podrá ser re-diseñado por el Operador. Deberá existir un utilitario para verificar las firmas digitales. El método de “timbre de agua” no será aceptado como prueba de autenticación, ya que modifica la grabación.

Almac*enamiento*

El sistema deberá mantener una cantidad configurable de video grabado en almacenamiento en línea. La cantidad de video almacenado en línea estará limitado por la capacidad de los Servidores de Cámara, en los cuales el espacio disponible para almacenar video en línea podrá ser configurable para cada unidad de disco.

El sistema deberá soportar RAID 0+1, 1, 3, 5 o 1+1 para grabación de video.

Adicionalmente el Servidor de Cámara deberá considera otros medios “off-line” de respaldo y restauración de video. Al menos uno de los siguientes dispositivos debe ser considerado:

- CD-RW.
- DVD-RW.
- Medios de almacenamiento USB.
- Medios Magnéticos.

Funciones de Operador

Para la integración de video, el software de aplicación debe considerar las siguientes funciones en la Estación de Operador:

- Visualizar video en vivo.
- Control PTZ.
- Visualización automática ante la ocurrencia de un evento.
- Búsqueda en los videos grabados de una cámara.
- Grabación Manual.
- Grabación de fotos de un video.
- Agregar una nueva cámara.
- Eliminar una cámara del sistema.
- Cambiar la configuración de una cámara.
- Grabación por evento/alarma.
- Búsqueda de video clips desde diferentes cámaras.
- Crear secuencias (tours de cámaras).
- Crear pantallas de cámaras múltiples.
- Configurar Video Analítico.
- Supervisión de cámaras.
- Manejo de entradas/salidas de cámaras (codificadores).
- Audio bi-direcional.
- Visualización de registros de auditoría.

Para la integración con control de accesos y alarmas, el software de aplicación debe considerar las siguientes funciones en la Estación de Operador:

- Reconocimiento de una alarma.
- Reset de alarmas.
- Control de un punto de seguridad.
- Reportes de información de seguridad.

La Estación de Operador deberá considerar texto en idioma español o permitir su traducción al español. Todo el texto que se despliega en las pantallas deberá estar almacenado en la base de datos de manera de permitir la traducción.

El software de aplicación deberá proporcionar la capacidad de desarrollo de aplicaciones locales para el acceso y control del sistema, utilizando una interface de desarrollo de aplicaciones. Estas aplicaciones podrán desarrollarse sin la necesidad de servicio del fabricante del sistema y se deberá proporcionar toda la documentación necesaria para su desarrollo.

SISTEMA DE CONTROL DE ACCESO

Descripción del Sistema

El Sistema de Control de Accesos tendrá una arquitectura Cliente-Servidor o a través de un acceso Web, basado en una red modular utilizando sistemas operativos estándar, redes y protocolos.

El Sistema tiene el objetivo de permitir un control seguro, rápido y eficiente de recintos estratégicos de la ANH, donde se mantengan procesos administrativos u operativos de importancia y que usos no autorizados podrían comprometer el normal funcionamiento del recinto.

El sistema permitirá, además de controlar el acceso a los recintos definidos como estratégicos o vulnerables, el registrar toda la actividad de acceso al recinto de manera de disponer de todo la información histórica que ayudaría a la investigación de eventos ocurridos en tal recinto.

Adicionalmente el sistema tendrá el objetivo de supervisar las puertas de estos recintos de manera de detectar acciones no permitidas, tales como, forzar la apertura de una puerta o mantener la puerta abierta.

La arquitectura general del sistema centralizado soportará servidores distribuidos de manera de permitir a sistemas múltiples e independientes, comunicarse entre sí para la transferencia de datos de manera de proveer una fácil y adecuada administración del sistema de seguridad y evitar la duplicidad de ingeniería.

El sistema centralizado permitirá la distribución de ciertas funciones del sistema, tales como la supervisión, control e interface gráfica de usuario, a través de toda la red de manera de permitir un máximo de flexibilidad y rendimiento.

La arquitectura del sistema deberá incluir el soporte de varias redes de área local (LAN y WAN) utilizando hardware y software estándar para enlazar nodos en un solo sistema integrado. El protocolo de red a utilizar deberá ser TCP/IP estándar.

El Sistema de Control de Accesos podrá ser operado y supervisado a través de cualquiera de sus Estaciones de Trabajo en una sesión con los permisos correspondientes.

Las principales aplicaciones del Sistema de Control de Accesos deberán incluir, como mínimo, las siguientes:

- Control de Accesos de áreas restringidas.
- Control de Recepción.
- Control de Rondas de Guardias.
- Credencialización.
- Administración de Seguridad para la Detección de Intrusos.
- Control de Bienes.
- Control horarios
- Control de visitas
- Acceso a través de biométrico.
- Control de ingreso a través de torniquetes.

El Control de Accesos estará basado en una identificación personal de funcionarios, colaboradores y visitas utilizando tarjetas de identificación del tipo inteligentes por proximidad compatibles con el control de acceso del edificio. La selección de tecnología para las tarjetas de control de accesos no podrá estar limitada, donde diferentes tecnologías deberán estar disponibles y además deberá permitir el cambio a tecnologías más seguras con el mínimo de implementación de nuevo hardware y software e impacto reducido en la base de datos.

El Sistema de Control de Accesos deberá considerar un módulo de generación de credenciales, y la posibilidad de instalar una impresora de tarjetas.

El proponente debe proporcionar la impresora de tarjetas y los insumos necesarios para imprimir 500 carnéts.

Este sistema podrá ser integrado con otros sistemas de seguridad, de manera de actuar en forma integral y automática. En caso de existir una alarma de incendios confirmada, el Sistema de Control de Accesos automáticamente liberará todas las puertas del sector alarmado que tengan cerraduras controladas por el sistema. El estado de cada puerta será supervisado por el servidor de control de accesos de manera de conocer si la puerta está abierta o cerrada, y generar las alarmas de supervisión de “puerta forzada abierta” o “puerta mantenida abierta”.

En la integración con el Sistema de Circuito Cerrado de Televisión, se considera una cámara de CCTV asociada a cada puerta controlada con lectores de proximidad, las cuales estarán grabando permanentemente la actividad en cada puerta. Esto toma relevancia en los períodos en que las puertas son liberadas en forma automática en

caso de una alarma de incendios, o cuando forzadamente son mantenidas abiertas, lo cual es reportado como una señal de supervisión.

El Sistema tendrá una administración centralizada donde se pueda configurar y controlar todo el sistema y además recibir las señales de supervisión y alarmas.

Operación del sistema de control de accesos

Para ingresar a un recinto con acceso controlado, el funcionario y contratista, deberá presentar su tarjeta personal al lector ubicado en la entrada del recinto, asimismo, en algunas puerta defendías como críticas se deberá autenticar de manera biométrica.

Si la persona está autorizada en el sistema, se permitirá el acceso a través de un torniquete o apertura de puerta, permitiendo el ingreso de la persona. Si la persona no está autorizada para ingresar a ese recinto, el sistema permanecerá cerrado.

Al presentar una tarjeta autorizada o accionar el pulsador de salida, la Unidad de Control destrabará la puerta y permanecerá destrabada por algunos segundos, después de lo cual se energizará nuevamente. Al mismo tiempo la Unidad de Control inhibirá al sensor de puerta durante algunos segundos permitiendo que la puerta se abra sin dar una condición de alarma. Transcurrido el tiempo necesario para que la puerta vuelva a su posición de cerrada, el contacto entrará en su estado activo y originará una alarma local si la puerta aún permanece abierta después de haber transcurrido el tiempo de apertura. Los tiempos de apertura de cada puerta son ajustables por programación.

Todas las puertas controladas por el sistema, deben poseer un sistema de cierre automático de la puerta mediante un quicio automático de cierre y control de fuerza. Si la puerta no considera quicios, entonces se debe considerar un brazo de cierre hidráulico en la parte superior.

Cada transacción ocurrida en la puerta, se registrará y almacenará toda la información relacionada con el evento:

- Hora y fecha.
- Tipo de transacción.
- Nombre del Usuario de Tarjeta.
- Nº de tarjeta.
- Identificación del punto donde ocurre (puerta, punto de entrada o salida).

Al recibir la señal de la lectora activada por una tarjeta, o la acción de un pulsador de salida, la Unidad de Control llevará a cabo las siguientes acciones siempre y cuando la tarjeta tenga acceso permitido y esté en el horario autorizado:

- Accionar el relé de control de chapa para des energizar y liberar la puerta. Este relé permanecerá activado por un tiempo programado por el usuario, necesario para que la persona abra la puerta.
- Inhibir la acción del sensor de estado de la puerta, durante el tiempo programado por el usuario. En aquellas puertas que deban permanecer abiertas por mucho tiempo, esta función estará desconectada y el sensor sólo cumplirá la función de monitorear el estado y registrarlo cada vez que éste cambie.
- Generar una señal de alarma cuando se produzca una de las siguientes transacciones no autorizadas:
  - Intentar regresar por una puerta con acceso denegado.
  - Tratar de ingresar por una puerta fuera del horario autorizado a esa tarjeta.
  - Mantener una puerta abierta por un tiempo mayor al programado.
  - Forzar una puerta hasta abrirla sin autorización.

En caso de que una tarjeta sea usada en una lectora en la cual el usuario no tiene acceso o en un horario en el cual no le está permitido ingresar, el sistema deberá registrará la lectura en la base de datos incluyendo el resultado de la transacción, en la cual en este caso, deberá indicar acceso denegado por estar fuera de horario o simplemente porque no tiene acceso por esa puerta.

En caso de que una señal de alarma generada por un acceso forzado o por el sensor de puerta que ha detectado la puerta abierta más tiempo del permitido, el sistema responderá accionando un dispositivo audible localmente, que sólo podrá ser silenciado desde una Estación de Trabajo o al normalizarse esta situación.

Interacción con otros sistemas

Este sistema de control de accesos podría ser integrado con el Sistema de Control centralizado del edificio, y con otros sistemas de seguridad, de manera de actuar en forma integral y automática.

En caso de existir una alarma de incendios confirmada, el Sistema de Control de Accesos automáticamente liberará todas las puertas del sector alarmado que tengan cerraduras controladas por el sistema. El estado de cada puerta será supervisado por el servidor de control de accesos de manera de conocer si la puerta está abierta o cerrada.

De igual manera existirá una interrelación entre el Sistema de Control de Accesos y el Sistema de Circuito Cerrado de Televisión (CCTV), de manera que cuando exista una situación de supervisión o alarma en alguna de las puertas de control de accesos, en forma automática se visualizará la imagen de la cámara asociada a la puerta, en el caso

de existir, en una de las Estaciones de Trabajo en la Sala de Control, donde se registrará los datos del evento con las imágenes asociadas.

Al re-establecer el sistema de incendios a operación normal, la señal de alarma se elimina y el Sistema de Control de Accesos vuelve a operación normal controlando las puertas. El Sistema de Control de Accesos registra todos los eventos, tanto normales de accesos a las puertas, como las situaciones de alarmas externas, en el registro de eventos en el servidor del sistema.

Arquitectura del Sistema

La arquitectura deberá permitir tres niveles de procesamiento y control:

- **Nivel de Supervisión:** Presentación de estado y alarmas, interface hombre-máquina (parámetros de aplicación, configuración del sistema y control del sistema), y administración de datos históricos (eventos, valores y tráfico)

- **Nivel Periférico:** Nivel de decisión y retro-alimentación, compuesto de controladores inteligentes, cada uno con su propia base de datos y capacidad de comunicación entre ellos y con el servidor.

- **Nivel de Terreno:** Nivel donde el sistema interactúa con el "mundo externo" (empleados, visitas, puertas, detectores, etc,). Nivel compuesto de lectores, displays, teclados, actuadores, sensores, etc.

La configuración del sistema deberá asegurar la operación en situaciones y ambientes críticos. Se deberá aplicar redundancia a nivel servidores y nivel comunicaciones.

El o los Servidores de Control de Accesos, las Estaciones de Trabajo y Controladores deberán conectarse a una red de área local (LAN) estándar IEEE802.3, mediante cableado de cobre o fibra óptica.

El Sistema de Control de Acceso estará conformado por un Software de aplicación instalado en uno o más servidores, software de clientes instalados en estaciones de trabajo, enlaces de comunicaciones TCP/IP, controladores inteligentes, controladores de puertas, módulos de entradas y salidas, lectores y dispositivos de control y de supervisión.

La cantidad de cada uno de los equipos y dispositivos que conforman el sistema de control de accesos, dependerá de la cantidad de accesos y puntos de supervisión definidos en el proyecto.

La comunicación entre los controladores inteligentes y el servidor deberá ser en protocolo TCP/IP (Ethernet), dependiendo de la estructura del proyecto corrientes

débiles. La comunicación entre los controladores inteligentes y los controladores de puertas y módulos de supervisión se deberá realizar en protocolo TCP/IP o RS485, donde el alambrado deberá ser parte del proyecto de seguridad.

El servidor de bases de datos provee la administración y control centralizado de todos los datos del sistema y el o los servidores de comunicaciones administran y controlan todos los canales de comunicaciones con los controladores inteligentes distribuidos en la instalación.

El módulo de cliente permite a un Operador observar, controlar y mantener la operación del sistema de administración de seguridad. Esto incluye ver la actividad del sistema, registrar alarmas, reconocimiento de eventos y generar las acciones que resulten necesarias. En particular permite registrar la actividad de cada uno de los portadores de tarjetas programados en el sistema y controlar en forma segura el estado y actividad de cada acceso controlado.

Cada puerta con acceso controlado debe considerar según se haya definido en la necesidad de control de puerta el siguiente equipamiento:

- Lector de tarjetas por el lado de ingreso al recinto (para entrar).
- Lector biometrico
- Pulsador de apertura (REX) en el lado interior del recinto (para salir).
- En casos particulares, a definir en el proyecto, se deberá considerar lectores de tarjetas tanto en la entrada como en la salida.
- Pulsador de apertura en el interior de recintos
- Botón Desbloqueador de Emergencias en recintos con doble lector de accesos.
- Cerradura Electromagnética en cada hoja de la puerta.
- Supervisión del estado de la puerta (incluida en la cerradura).
- Accesorios de montaje de la cerradura de acuerdo a cada tipo de puerta.
- Fuente de poder independiente al Controlador, con batería de respaldo, 12V 4Ah.
- Brazo hidráulico para cierro autónomo de puerta.

Software de Control de Accesos

El software de Control de Accesos deberá ser instalado en un servidor basado Windows Server 2008 o superior, con aplicación real de 64 bits

Los servicios soportados por el servidor de control de accesos deben ser los siguientes:

- Soporte Multi-Usuario y Multi-Tarea.
- Soporte Red TCP/IP.

- Editor de Display Gráfico.
- Servicio de Base de Datos Microsoft SQL Server® 2008 o superior.
- Software de Aplicación.

El software de aplicación de Control de Accesos estará compuesto de diferentes módulos que, de acuerdo a las necesidades, se deberán instalar en uno o en varios equipos, Servidor de Base de Datos, Servidores de Comunicaciones, Estación de Trabajo con la aplicación de cliente, y otros servidores de aplicaciones si es necesario, de acuerdo a requerimientos de integración.

El software de control de accesos permite al operador administrar y configurar el sistema de control de acceso y la red de comunicaciones. Esto incluye la configuración del hardware, agregar/quitar usuarios, agregar/quitar tarjetas, cambiar códigos de autorización y definir, programar y activar todas las posibilidades de funciones operativas que permite el sistema.

Las principales características mínimas a cumplir el software de aplicación del programa de control de accesos, son las siguientes:

- Módulo de control de Acceso y control de horarios
  - Control de horarios
  - Configuraciones de novedades de funcionarios (Vacaciones, permisos, horas extras).
- Módulo de Control de visitas
  - Registro de Personas Visitante
  - Identificación de persona a quien se visita
  - Equipos electrónicos que ingresa
  - Definición de rutas seguras.
- La solución debe la opción de exportar los reportes de control de acceso, visitas, horarios, privilegios entre otros.
- Configuración Servidor/Cliente o Visualización Web.
- Compatible Microsoft, ambiente Windows.
- Comunicaciones en red TCP/IP con los Controladores Inteligentes.
- La Base de Datos de la solución debe ser preferiblemente Oracle, deseable Microsoft SQL Server 2008 o superior. En versiones de 64 bits.
- Debe permitir la importación y exportación de datos de usuarios.
- Debe permitir todas las tecnologías en los lectores, incluyendo biometría y tarjetas inteligentes.
- Debe permitir el uso de varias tecnologías de lectores en forma simultánea.
- Supervisión y control de entradas y salidas de alarma.
- Funciones de Antipassback, Two Man Rule, Esclusa.
- Capacidad gráfica de planos. Importación archivos CAD, JPG, BMP.
- Integración a nivel superior de Control centralizado.
- Integración con Sistema de CCTV.
- Integración con Sistema de Alarmas.

- Supervisión del sistema en tiempo real.
- Amplia capacidad de reportes configurables por el Operador.
- Debe permitir Auditoria del Sistema y de la Base de Datos.
- Debe considerar un módulo de software para le generación de credenciales.
- Debe permitir la conexión de una Impresora de Credenciales.
- La administración de las cuentas de usuario se debe integrar con las políticas de manejo de claves del LDAP de Colombiana de Comercio S.A. Adicional, se debe conectar al Directorio Activo de la compañía y permitir el manejo de esquemas Single Sign On.
- La solución no debe permitir que el usuario pueda alterar la información por base de datos. Cambios por panel.
- La solución debe permitir la automatización de copias de seguridad utilizando las características del administrador corporativo de SQL Server u Oracle.
- La aplicación debe permitir que a través de parametrizaciones o configuraciones del aplicativo, el usuario pueda determinar el comportamiento o funcionalidad requerida sin necesidad de modificar los programas que conforman la aplicación. En parámetros críticos debe ofrecer funcionalidad de control dual (una persona autorizada configura y otra autorizada aprueba).
- La solución debe contener un módulo centralizado de seguridad y control de accesos, que permita la asignación de roles y perfiles de usuario por cada opción del aplicativo.
- La solución debe permitir generar consultas y reportes en línea exportables a Excel, de los registros de las marcaciones realizadas por el personal dentro y fuera de las instalaciones de la compañía donde exista la terminal lectora.
- La solución debe permitir generar consultas y reportes en línea exportables a Excel, por: Gestor de Tiempos y por rango de tiempo determinado. Los reportes identificados son:
    - Marcación vs. turnos programado
    - Domingos descansados y laborados
    - Festivos descansados y laborados
    - Horas extras acumuladas
    - Cambios en el turno programado (cantidad y justificación)
    - Días compensados (fecha y cantidad)
    - Cantidad de veces que un empleado ha sido programado en un mismo turno.
    - Historial de turnos programados a una persona

Para el caso del software de las estaciones de Trabajo, se deben considerar las siguientes características básicas:

- Windows® 7 profesional 64bit o superior
- Red TCP/IP.
- Editor de Display Gráfico.
- Software de Aplicación.

El software de red de los servidores y de las estaciones de trabajo, deberán utilizar el protocolo estándar TCP/IP.

Especificaciones de Equipamiento

Controlador Inteligente

Los Controladores maestros periféricos deberán ser del tipo “inteligente”, basado en microprocesadores, con interfaces nativas a la misma red de área local de los Servidores y Estaciones de Trabajo.

El Controlador inteligente y flexible y estar basado en un procesador CPU de 32 bits, con opción de protocolo TCP/IP, firmware en memoria flash, base de datos local de usuarios de gran tamaño, gran capacidad para controlar módulos de lectores y de entrada y salida.

El Controlador Inteligente debe permitir el funcionamiento fuera de línea, sin comunicaciones con el servidor, y permitiendo que las decisiones de control de acceso se puedan tomar en forma independiente de un software central u otro dispositivo de control. También puede ser conectado a un equipo servidor con el software de control de accesos, para la configuración del sistema, monitoreo de alarmas y control directo.

La conectividad al servidor debe permitir la conexión mediante protocolo TCP/IP para la interconexión a través de redes Ethernet.

El Controlador Inteligente debe soportar cualquier combinación de hasta 32 módulos de lectores o de entrada/salida, de manera de monitorear puntos de alarma, salidas de relés, o puntos con interfaces para lectores de control de accesos.

El Controlador Inteligente debe tener una capacidad mínima de 20.000 tarjetas y posibilidad de ampliación a 100.000 tarjetas a través de la ampliación de la memoria. Adicionalmente debe disponer un buffer con capacidad mínima de 5.000 transacciones y posibilidad de ampliación a 35.000 registros.

El módulo de controlador inteligente podrá ser montado en muro (en gabinete) o en gabinete adecuado para permitir una máxima densidad.

Controlador de Puerta

El módulo Controlador de Puertas se deberá interconectar con el Controlador Inteligente a través de conexión Ethernet con protocolo TCP/IP, o mediante un bus RS485 a 38.400bps, y debe disponer de dos puertas para lectores de formato wiegand, un mínimo de 8 entradas supervisadas y 6 salidas de relé. Se debe disponer además de la alternativa de un módulo Controlador con una sola puerta de lector para los casos en que no sea necesario disponer de dos lectores.

El Controlador de puertas debe permitir el uso de lectores de diversas tecnologías, incluyendo como mínimo banda magnética, código de barras, proximidad, teclado, biométrico y tarjeta inteligente. Debe permitir la supervisión del estado de la puerta (abierta/cerrada).

Toda la configuración del Controlador, incluyendo el formato de las tarjetas, es descargada desde el Controlador Inteligente conectado.

Puerta abierta / cerrada supervisión. En el caso de que la comunicación a un Controlador Inteligente se pierde, el controlador de puertas puede conceder el acceso basado en la utilización de código de sitio, acceso denegado o acceso libre.

Las características de los controladores de puertas deberán ser las siguientes:

- Entrada de 2 lectores - 12 VDC at 50 mA.
- Formato Wiegand.
- Capacidad de integración de un Teclado de Código.
- Datos de Teclado multiplexado con datos de la tarjeta.
- Soporte de control de LED bicolor.
- Mínimo de 8 entradas supervisadas de alarma.
- 2 entradas de alarma dedicada a tamper y pérdida de energía.
- 2 salidas de relé de propósito general Form C. 5A 28VDC.
- 4 salidas de relé de propósito general Form C. 2A 28VDC.
- Cargador de Baterías incorporado.
- Supervisión Estado de puerta.
- Entrada para pulsador de salida.

Cada transacción almacenada deberá contener al menos la siguiente información:

- Hora y fecha.
- Tipo de transacción.
- Nombre del Usuario de Tarjeta.

- Nº de tarjeta.
- Identificación del punto donde ocurre (puerta, punto de entrada o salida).

Al recibir la señal de la lectora activada por una tarjeta, o la acción del botón desbloqueado, la Unidad de Control llevará a cabo las siguientes acciones siempre y cuando la tarjeta tenga acceso permitido y esté en el horario autorizado:

- Accionar el relé de control de chapa para des energizarla y liberar la puerta. Este relé permanecerá energizado por un tiempo programado por el usuario, necesario para que la persona abra la puerta.
- Inhibir la acción del sensor de estado de la puerta, durante el tiempo programado por el usuario. En aquellas puertas que deban permanecer abiertas por mucho tiempo, esta función estará desconectada y el sensor sólo cumplirá la función de monitorear el estado y registrarlo cada vez que este cambie.
- Generar una señal de alarma cuando se produzca una de las siguientes transacciones no autorizadas:
  - Intentar regresar por una puerta con acceso denegado.
  - Tratar de ingresar por una puerta fuera del horario autorizado a esa tarjeta.
  - Mantener una puerta abierta por un tiempo mayor al programado.
  - Forzar una puerta hasta abrirla sin autorización.

- En caso de que una tarjeta sea usada en una lectora en la cual el usuario no tiene acceso o en un horario en el cual no le está permitido ingresar, el sistema deberá responder del siguiente modo:
  - Registrará la lectura en la base de datos incluyendo el resultado de la transacción, en la cual en este caso, deberá indicar acceso denegado por estar fuera de horario o simplemente porque no tiene acceso por esa puerta.
- En caso de que una señal de alarma generada por un acceso con fractura o por el sensor de puerta que ha detectado la puerta abierta más tiempo del permitido, el sistema responderá accionando un dispositivo audible localmente, que sólo podrá ser silenciado desde una Estación de Trabajo o al normalizarse esta situación.
- El sistema deberá tener la capacidad de destrabar las puertas en forma automática, si el sistema de detección de incendio se activa.

Lector biométrico

Los lectores de controles de accesos biométricos (huella) deberán tener tecnología de proximidad para tarjetas "inteligentes", para un control más poderoso, versátil y con seguridad mejorada a través de la encriptación de datos y autentificación mutua entre la tarjeta y el lector.

Adicionalmente debe tener las siguientes especificaciones técnicas:

- Lectura de huella menos de 1 segundo.
- Margen de error no mayor a un 5%, por la cantidad de lectura en los DPI, en ambientes de oficina disminuye hasta un 1%.
- Captura de algoritmo y no una imagen como lector óptico.
- Especialmente adecuado para interiores.
- Resolución 508 dpi
- Área sensitiva 12.8 x 18mm o superior

Lector de accesos

Los lectores de controles de accesos deberán ser de tecnología de proximidad para tarjetas "inteligentes", para un control más poderoso, versátil y con seguridad mejorada a través de la encriptación de datos y autentificación mutua entre la tarjeta y el lector.

Los lectores de control de accesos para tarjetas inteligentes tendrán las siguientes características principales:

- Compatibilidad de Formatos. Permite la utilización de mismos formatos de las tarjetas de proximidad estándar.
- Seguridad. Toda la transmisión de data mediante señal RF entre la tarjeta y el lector es encriptada mediante un algoritmo seguro. Utilizando técnicas de encriptación estándar de la industria y administración avanzada de códigos de 64 bits, la tecnología de tarjetas inteligentes reduce el riesgo de pérdida de datos o duplicidad de tarjetas.
- Operatividad. Los tarjetas deberán cumplir estándar de operación ISO con compatibilidad con variadas tecnologías de tarjetas (ISO 15693, ISO 14443A e ISO 14443B).
- Rango de Lectura Asegurado. Mediante técnicas de auto-sintonía se ajusta automáticamente el lector para un funcionamiento optimizado en cualquier superficie de montaje.

- Indicación Audiovisual. Mediante un buzzer incorporado se generan varios tonos para indicar acceso autorizado, acceso negado, alimentación de energía y diagnósticos. Una barra iluminada de alta intensidad proporciona una indicación visual del estado del lector.
- Fácil integración. El lector tendrá salida en formato wiegand lo que le permitirá conectarse a la mayoría de Controladores de Accesos con protocolos wiegand y "Clock and Data". El Lector se podrá configurarse para generar salidas en formato wiegand de 26 bits, 32 bits, 34bits, 40 bits o 56 bits basados en el número serial de las tarjetas.
- Diseño para uso interior/exterior. Fabricación en un gabinete de policarbonato para uso en exteriores, permitiendo su funcionamiento seguro en ambientes adversos y resistencia al vandalismo.

Tarjetas "Inteligentes" para Control de Accesos

El proponente debe entregar cuatrocientas 400 tarjetas lectoras a las ANH, como entregable del sistema.

Las tarjetas para el control de accesos deberán ser de tecnología "inteligente" de proximidad, con tecnología NFC de largo alcance y podrán ser utilizadas en diversas otras aplicaciones, tales como, biometría, control de asistencia, accesos a computadores e impresoras y redes, casinos, transporte, y aplicaciones diseñadas por el cliente. Archivos múltiples, separados con seguridad incorporada, permite numerosas aplicaciones y soporta crecimiento futuro.

Las tarjetas utilizarán una frecuencia de 13.56MHz para la transmisión de datos con los lectores, y permitirán la incorporación de bandas magnéticas, códigos de barras, proximidad estándar, y la impresión directa de datos y fotos del usuario (credenciales).

Las tarjetas "inteligentes" de control de accesos tendrán las siguientes características principales:

- Comunicaciones. Tecnología de transmisión en 13.56MHz para lectura y escritura, permite alta velocidad, integridad y seguridad en las comunicaciones
- Seguridad. La tecnología de tarjeta "inteligente" garantiza una alta seguridad con autentificación mutua entre el lector y tarjeta, transferencia encriptada de datos y códigos de 64 bits
- Codificación. Cualquier código puede ser programado en fábrica en un área de aplicación de control de accesos
- Memoria. Alternativas de configuración de 2k bit (256 bytes), 16k bit (2K Byte) o 32k bit (4K Byte)
- Dimensiones y peso. 5.40 x 8.57 x 0.084 cms, 5.7 grs
- Fabricación. Tarjeta delgada, flexible laminada en PVC

Pulsador de salida.

De acuerdo a la clasificación de Nivel de Seguridad de cada recinto, en los accesos de alto nivel de seguridad se ha definido la utilización de lectores para la entrada y lectores para la salida. En el resto de los recintos solo se considerará lector para el ingreso a cada recinto, donde por el lado interior del recinto se instalará un pulsador normalmente abierto que permita abrir la puerta desde el interior sin usar la tarjeta. En este caso específico no se requiere el control de salida, razón por la cual cada egreso sólo quedará registrado como el accionamiento del pulsador sin identificación de la persona.

Al accionar el pulsador de salida, la Unidad de Control destrabará la puerta y permanecerá destrabada por algunos segundos, después de lo cual se energizará nuevamente. Al mismo tiempo la Unidad de Control inhibirá al sensor de puerta durante algunos segundos permitiendo que la puerta se abra sin dar una condición de alarma. Transcurrido el tiempo necesario para que la puerta vuelva a su posición de cerrada, el contacto entrará en su estado activo y originará una alarma local si la puerta aún permanece abierta después de haber transcurrido el tiempo de apertura. Tanto el tiempo de destrabamiento y el tiempo de apertura de la puerta son ajustables por programación.

El Pulsador de Apertura será de “agradable” aspecto, construcción sólida y larga duración, y deberá estar supervisado por el sistema de control de accesos.

Botón Desbloqueador

Al accionar el botón desbloqueador, la Unidad de Control destrabará la puerta en forma constante hasta que el botón sea repuesto manualmente. Al estar el botón y la puerta permanentemente supervisada, se generará una alarma en el sistema centralizado cuando la puerta sea desbloqueada por este botón.

El Botón Desbloqueador deberá ser del tipo normalmente cerrado con retención mecánica, tipo hongo, larga duración, “agradable” aspecto, protección externa transparente de manera de evitar accionamientos involuntarios o mal intencionados, con leyendas claras que indiquen el carácter de uso solo en caso de emergencias.

Cerraduras Electromagnéticas (Electroimanes)

Se debe proponer cerraduras del tipo electromagnético con un sensor de supervisión incorporado que sólo se accione cuando la puerta esté en la posición cerrada y segura.

La cerradura deberá poseer las siguientes características técnicas:

- Fuerza de retención : 600 Lbs.
- Voltaje de operación : 12/24 VDC.
- Indicador de estado : Contacto tipo C interno.
- Construcción : Apta para interior y exterior.
- Rango de Temperatura : -40 ºC a +60 ºC.

Se debe considerar que todas las puertas controladas por el sistema, deben poseer un sistema de cierre automático de la puerta mediante un quicio automático de cierre y control de fuerza. Si la puerta no considera quicios, entonces se debe considerar un brazo de cierre hidráulico en la parte superior.

Control de paso de personas (Torniquetes)

Se debe implementar un sistema de control de acceso a las oficinas de la ANH desde la entrada principal ubicada en la recepción de segundo piso, que evite el ingreso de personal que no se autentique a través de lector biométrico.

- Gabinete mono block totalmente, hecho en acero inoxidable AISI 304, con1,5 mm de espesura, resistente a choques, vibraciones, elementos ácidos y alcalinos.
- Brazos en tubos de acero. con refuerzo interno en acero carbono, roscados en el cabezal y fijados con tornillos de difícil acceso.
- Mecanismo provisto con sistema de trabado, en caso de falta de energía, destraba el equipo, para atender normas de seguridad (Emergency Sysfem).
- Todas las piezas mecánicas deben ser tratadas contra la corrosión por el proceso de bicromatizado trivalente, según la directiva RoHS.
- Bloqueo del giro por el sistema de enclavado a través de dos triques Y dos solenoides (Double Lockl, que controlan el flujo de usuarios de forma independiente (entrada y salida).
- Capacidad de soporte de bloqueo de una persona de 120 Kg a 5 Km/h.

<u>Es importante implementar un mecanismo que permita el ingreso a personas en estado de discapacidad y que por su condición no puedan pasar por los torniquetes.</u>

Impresoras de carnets PVC

El proponente debe entregar una impresora de carnet en PVC para la impresión de tarjetas de control de acceso con las siguientes características:

- La impresora deber imprimir sobre tarjetas PVC de control de acceso.

- La impresora deber imprimir los adhesivos que se pegan a las tarjetas PVC de control de acceso.
- Tarjeta directa de sublimación de tinta / transferencia térmica de resina.
- Impresión a una cara, con el borde de borde a •
- Estándar de 300 x 300 DPI de resolución.
- Personalizable 300 x 600 PPP (color e impresión monocromática) o 300 x 1200 dpi de resolución (Sólo impresión monocromática).
- 32 MB de memoria (RAM) estándar - opcional 64 MB1
- Impresión de un solo lado: - Color (YMCKO) : 190 - 225 tarjetas / hora - Monocromo : 800 - 1000 tarjetas / hora
- Lado dual: - Color (YMCKO - K) : 140 tarjetas / hora
- USB (1.0 , 1.1 , 2.0 , 3.0) , el cable suministrado
- Ethernet TCP - IP 10BaseT , 100BaseT (LED de tráfico)
- Conexión inalámbrica 802.11b / g en el rango inalámbrico

Fuentes de Poder

La alimentación de las cerraduras electromagnéticas será en forma separada e independiente de los Controladores de Accesos. Se proveerá Fuentes de Poder con baterías que permitan una autonomía de 6 horas de funcionamiento en caso de corte de energía. La fuente de poder deberá mantener las baterías a flote y a plena carga cuando el sistema esté bajo régimen normal.

Canalización y alambrado

- El proyecto de Corrientes Débiles considera la instalación de bandejas de corrientes débiles a través de todos los recintos, pasillos y áreas comunes. El instalador del Sistema de Control de Accesos deberá canalizar todos los elementos desde cada puerta controlada hasta las bandejas de corrientes débiles más cercanas disponibles, lo cual se podrá ejecutar en ducto EMT de ¾".

- El Cableado a considerar desde cada elemento de control de accesos, hasta los controladores, deberá corresponder a los requerimientos del fabricante de los equipos de control de accesos. Como referencia debe ser con las siguientes características:

  - Lectores: Cable Multifilar de 5 conductores calibre mínimo 20AWG con blindaje total.
  - Pulsadores: Cable duplex 2*20AWG.
  - Cerraduras: Cable duplex polarizado 2 x 18AWG.

- Para la comunicación entre controladores de puertas se deberá considerar cable de comunicaciones 2 x 18AWG blindado. Para la comunicación en red desde el Controlador Inteligente hasta el punto de red, se deberá considerar cable de red Categoría 6.

Sistemas de alarmas

Se debe considerar la instalación de sistemas de alarmas locales, y supervisados por el sistema centralizado de seguridad, como complemento a los sistemas de control de accesos y de circuito cerrado de televisión que poseen estos recintos. El objetivo de estos sistemas de alarma es proveer de un sistema de detección de intrusos cuando los recintos permanecen sin personal autorizado.

Los elementos y dispositivos de detección de intrusos, tales como, contactos magnéticos para la supervisión de las puertas y sensores infrarrojo interior, se pueden revisar para presentar como solución de acuerdo a la distribución de seguridad que se quiera plantear en los planos.

Todos los equipos, dispositivos y elementos especificados en este documento deberán estar aprobados por un organismo internacional, tal como UL u otros, salvo que se indique lo contrario en estas especificaciones

El sistema deberá incluir, pero sin limitarse a, los siguientes elementos:

- Panel De Control
- Fuente de Poder
- Loop de Comunicaciones
- Teclado de Programación y Operación
- Baterías
- Contactos Magnéticos
- Sensores de Movimiento
- Canalizaciones y Alambrado
- Cualquier otro componente necesario para una adecuada operación del sistema.

El sistema deberá estar listado como Dispositivo de Potencia Limitada y listado de acuerdo a los siguientes estándares:

UL 609 “Sistemas Locales de Alarma contra Robo”
UL 1635 “Sistema de Comunicaciones Digitales de Alarma”

El panel de control deberá posee las siguientes características técnicas:

- Las áreas y zonas del sistema deberán ser programables y permitir ingresar leyendas del cliente para identificar a las áreas, zonas y usuarios.

- El Sistema deberá permitir compatibilidad integrada con equipamiento de expansión de zonas de tecnología alámbrica y/o inalámbrica.
- El Sistema deberá permitir la conexión de teclados de operación, módulos de expansión de zonas, módulos de zonas inalámbricas, controladores,
- Los relés de salida podrán ser programados para una acción momentánea, continua, pulsada o como seguimiento del estado de una zona de entrada asociada.
- El Sistema podrá ser completamente programable localmente a través de un teclado o un Computador, o remotamente a través de una conexión en red LAN, WAN o Internet.
- La Unidad de Control deberá estar equipada con un elemento automático para prevenir el daño debido a una conexión reversa accidental de los cables de batería.
- El Panel de Alarma deberá permitir la integración con el sistema de control de accesos del recinto y también con el sistema de control centralizado.

Puertas a controlar

A continuación se describe la cantidad de elementos que el contratista debe proporcionar para el control de puertas según las necesidades definidas por la ANH

Puerta	Piso	Descripción de Puerta	Torniquetes	Biométricos	Lectora	Electroimanes	Contacto Magnético	Botón de Salida	Brazo Hidráulico	Observaciones
1	1	Entrada radicación	0	0	0	1	1	0	1	
2	2	Entrada Principal	3	2	0	1	1	1	0	Dos (2) para acceso personal uno (1) para acceso de discapacitados.
3	2	Puerta de Vidrio (camino hacia auditorio)	0	0	1	1	1	1	1	
4	2	Recepcion EPIS	0	1	0	1	1	1	1	
5	2	Cuarto Eléctrico	0	0	1	1	1	1	1	

Puerta	Piso	Descripción de Puerta	Torniquetes	Biométricos	Lectora	Electroimanes	Contacto Magnético	Botón de Salida	Brazo Hidráulico	Observaciones
6	2	Acceso Vice Técnica (Ascensor)	0	0	1	1	1	0	0	
7	2	CCP- Entrada	0	1	1	1	1	0	1	
8	2	CCP- Salida	0	0	0	0	1	0	1	
9	3	Acceso de ascensores	0	2	0	1	1	0	1	
10	3	Cuarto Eléctrico	0	0	1	1	1	1	1	
11	3	Archivo 472	0	1		1	1	1	1	

Puerta	Piso	Descripción de Puerta	Torniquetes	Biométricos	Lectora	Electroimanes	Contacto Magnético	Botón de Salida	Brazo Hidráulico	Observaciones
12	3	Archivo 472 (Cafetería)	0	1	0	1	1	1	1	
13	3	Acceso Recepción Presidencia	0	1	1	1	1	0	1	
14	3	Acceso Recepción Presidencia (Ascensor)	0	1	0	1	1	1	1	
15	3	Acceso Oficina Presidencia (Ascensor)	0	1	0	1	1	1	1	
16	4	Cafetería	0	0	0	1	1	1	0	
17	4	Entrada a GYM (Puerta de Vidrio)	0	0	0	0	0	0	0	

Puerta	Piso	Descripción de Puerta	Torniquetes	Biométricos	Lectora	Electroimanes	Contacto Magnético	Botón de Salida	Brazo Hidráulico	Observaciones
18	4	Acceso exterior Puerta grande	0	1	0	1	1	1	1	
19	4	Archivo 4-72	0	1	0	1	1	1	1	
20	4	Recepción 4-72	0	0	2	1	1	1	1	
21	4	Acceso exterior Puerta Pequeña	0	1	0	1	1	1	1	
		Total Elementos:	**3**	**14**	**8**	**19**	**20**	**14**	**17**	

SERVICIOS

Instalación y parametrización

EL contratista deberá implementar el 100% de la infraestructura tecnológica asociada con el control de acceso y CCTV, así como la parametrización del sistema en un plazo no mayor a sesenta días calendario a partir de la firma del acta de inicio.

Garantía

El Contratista garantizará todas las labores, mano de obra especializada, materiales y el buen funcionamiento del Sistema de Control de Accesos y CCTV, por un periodo de tres años a partir de la firma de acta de inicio. Si una falla ocurre en este periodo el Contratista proporcionará toda la mano de obra y materiales necesarios para la reposición satisfactoria del sistema.

Mantenimientos preventivos y correctivos

Mantenimiento Preventivo

Realizar un (1) mantenimientos preventivo cada tres (3) meses a todo el sistema de seguridad electrónica (CCA y CCTV) en la ejecución del presente contrato (tres (3) años), realizando el primer mantenimiento en un término no mayor a los tres (3) meses después de firmada el acta de inicio.

Mantenimiento Correctivos

Realizar los mantenimientos correctivos que sean necesarios al sistema de seguridad electrónica (CCA y CCTV), en un tiempo no mayor a ocho (8) calendario una vez se haya reportado la falla.

ANEXO 2 – PROPUESTA ECONÓMICA
(FAVOR NO MODIFICAR NINGUN ÍTEM O DESCRIPCIÓN NI CANTIDAD)

ÍTEM	DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
1	**SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)**			
1.1	Servidores de Base de Datos.	1	COP -	COP -
1.2	Servidores de Cámaras (Almacenamiento)	1	COP -	COP -
1.3	Multiprocesamiento y Tolerancia a Fallas	1	COP -	COP -
1.4	Estaciones de Operador	1	COP -	COP -
1.5	Teclados de Operador	1	COP -	COP -
1.7	Cámara Fija Interior tipo Mini-Domo	38	COP -	COP -
1.8	Cámara 360°	24	COP -	COP -
1.9	Red Ethernet y Cableado de Red.	1	COP -	COP -
1.10	Canalizaciones y Alambrado	1	COP -	COP -
1.11	Software de Aplicación	1	COP -	COP -
2	**SISTEMA DE CONTROL DE ACCESO**			
2.1	Software de Control de Accesos	1	COP -	COP -
2.2	Controlador Inteligente	1	COP -	COP -
2.3	Controlador de puerta	1	COP -	COP -
2.4	Lector Biométricos	14	COP -	COP -
2.5	Lectora de tarjetas	8	COP -	COP -
2.6	Tarjetas inteligentes para control de Acceso	400	COP -	COP -
2.7	Botón de Salida	14	COP -	COP -
2.8	Botón desbloqueador	4	COP -	COP -

ÍTEM	DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
2.9	Cerraduras Electromagnéticas (Electroimanes) +Sensor	20	COP -	COP -
2.10	Fuentes de Poder para Cerraduras Electromagnéticas	20	COP -	COP -
2.11	Torniquete	3	COP -	COP -
2.12	Impresoras de carnets PVC	1	COP -	COP -
2.13	Canalización y alambrado	1	COP -	COP -
2.14	Control de acceso para discapacitados	1	COP -	COP -
2.15	Brazo hidráulico	17	COP -	COP -
2.16	Sistema de alarmas para puertas	21	COP -	COP -
3	**SERVICIOS**			
3.1	Instalación y parametración	1	COP -	COP -
3.2	Garantía (3 años)	1	COP -	COP -
3.3	Mantenimientos preventivos y correctivos (3 años)	1	COP -	COP -

PRECIO TOTAL:	**COP -**
IVA (16):	**COP -**
PRECIO TOTAL + IVA:	**COP -**