|  |  |  |  |
| --- | --- | --- | --- |
|  | **DESCRIPCION** | **CUMPLE SI/NO** | **OBSERVACIONES** |
| **Software** | El software de gestión de control de acceso deberá́ poseer como opción un sistema de enrutamiento TCP/IP secundario de Back Up por si la red principal de comunicación sufre alguna afectación.  Las características mínimas para el servidor principal y los PC clientes (Visitantes y PC de gestión remota), para la gestión de control de acceso deben ser core i3, RAM 4GB, Disco Duro 1TB (El servidor de gestión de control de acceso debe poder operar mínimamente con estas características).  Se recibirán equipos con mejores características sin embargo el software debe estar en la capacidad de operar fluidamente con las características anteriormente mencionadas.  Los equipos PC cliente deben ser tipo desktop pero que cumplan con las características anteriormente mencionadas.  El software de Gestión de control de acceso deberá́ ser compatible con sistemas operativos Windows en sus versiones 32 y 64 Bits para versiones Pro y Server. Específicamente Windows 10 Pro.  El software de gestión de control de acceso deberá tener arquitectura cliente – servidor y por lo menos 5 estaciones de trabajo incluidas.  El software de gestión de control de acceso deberá contar con una conexión remota por servicio Cliente Web desde un explorador de internet o aplicativo móvil que permita la gestión y programación en caso de emergencia desde un teléfono móvil inteligente previamente configurado para tal fin de ser necesario.  El software de gestión de control de acceso deberán poseer diferentes niveles de seguridad de acuerdo con los usuarios del sistema. |  |  |
| El software de gestión de control de acceso deberá́ contar con mapas interactivos donde se puedan utilizar formatos DGW de AutoCAD o en su defecto imágenes convencionales JPG o similares con el fin que desde estos mapas se pueda interactuar de manera remota con los diferentes puntos de acceso de manera gráfica.  El Software de gestión de control de acceso y sus demás componentes solicitados en el actual pliego de condiciones deberán ser de fabricantes reconocidos del mercado, con más de 10 años de experiencia en el mercado latinoamericano, no se aceptarán soluciones hechas a la medida y/o soluciones OEM.  El software de gestión de control de acceso deberá́ permitir la generación de reportes automatizados por evento o por agendamiento.  El software de gestión de control de acceso utilizará como motor de base de datos MS SQL el cual será instalado automáticamente con la instalación del software de gestión de control de acceso y deberá permitir el enrolamiento de por lo menos 256 Lectores. |  |  |
| El software de gestión de control de acceso deberá estar en la capacidad de realizar las siguientes funciones: 1. Comunicación a terceros por medio de una dirección IP y puerto especifico indicando eventos del sistema de manera paralela al diligenciamiento a la base de datos que utilice el sistema. 2. Diligenciamiento de una base de datos de terceros de manera paralela al diligenciamiento a la base de datos que utilice el sistema. 3. Integración a la fecha (No desarrollos posteriores) con lectores Biométricos Monomarca que utilicen la misma plataforma de gestión dentro del mismo software para crecimiento posterior en esta tecnología. 4. Carga masiva de base de datos otorgada por la Institución hacia el software de gestión de control de acceso. 5. Poseer en un licenciamiento a la fecha (No desarrollos posteriores) una forma de comunicación de protocolo abierto por IP - OPC para integración con terceros de ser necesaria. |  |  |
| El software de gestión de control de acceso deberá tener la capacidad de crecimiento ilimitado utilizando licenciamientos adicionales de ser necesarios en el futuro.  El software de gestión de control de acceso deberá tener desarrollado a la fecha el poder controlar puertas o puntos de acceso con y sin lector de manera remota de ser requerido en el futuro.  El software de gestión de control de acceso deberá poder operar de forma centralizada y remota, esto es, podrá configurar los controladores centralizadamente y podrá recibir los diferentes eventos desde los controladores remotamente.  El software de gestión de control de acceso deberá poder interconectar por medio de aplicativos monomarca, cámaras de video vigilancia IP de fabricantes de terceros, así la universidad no quedará atada a una sola marca de cctv.  El fabricante de la solucion de gestión de control de acceso en ese orden de ideas deberá contar con una solucion de Video Managment System con posibilidad de albergar por cada servidor por lo menos hasta 64 canales de cámara tomando un streaming de la cámara para tal fin.  Este VMS Video Managment System deberá poder integrarse de manera nativa con el sistema de gestión de control de acceso para que así, se puedan traer pop ups de cámara enlazados a eventos de acceso según demanda o por evento.  Sí se decidiera grabar estos canales de CCTV en el VMS ofertado monomarca con la solución de control de acceso ofertada, este deberá poder enlazar los eventos de acceso a eventos exactos de video histórico, pudiendo desde el mismo reporte de acceso tener la facultad de adquirir el evento de video histórico ocurrido. Se debe ofertar la licencia base para la integración solicitada, las licencias por canales de cámaras, si hay lugar a ellas, serán adquiridas en una segunda etapa.  El software de gestión de control de acceso deberá permitir la utilización de puertas virtuales en salidas de emergencia de ser requerido en el futuro. El software de gestión de control de acceso deberá́ tener la capacidad de crecimiento ilimitado utilizando licenciamientos adicionales de ser necesarios en el futuro. |  |  |
| El software de gestión de control de acceso deberá ser del mismo fabricante que el resto de los elementos que componen la arquitectura de diseño del sistema, incluyendo de manera concreta y puntual controladores maestros del sistema, software de visitantes y lectores del sistema.  El software de gestión de control de acceso deberá poder gestionar alarmas de eventos supervisados (eventos de control de acceso y eventos de contacto seco de ser necesario utilizando módulos adicionales de entradas y salidas ligados al sistema de control de acceso), y poder generar reportes de alarma históricas.  El software de gestión de control de acceso, debe poseer integración con Directorio Activo, esta debe ser ofertada en esta propuesta en cantidad unitaria a servidor.  El software de gestión de control de acceso deberá poseer una herramienta que permita el cargue masivo de tarjeta habientes y sus atributos (Niveles de acceso, fechas de terminación de permisos, creación de usuarios nuevos, eliminación de usuarios viejos, inhabilidad de tarjeta habientes, entre otros) por horario, cada tiempo estipulado y por demanda.  El software de gestión de control de acceso deberá poseer licenciamiento que permita integración con sistemas Building Management Systems BMS o similares por medio de OPC (OLE for Process Control), esto debe ser soportado por carta del fabricante directamente firmado por la persona representante de fábrica a nivel nacional (No canal distribuidor, Integrador u Oferente). |  |  |
| El software de gestión de control de acceso deberá contar con la opción de Antipassback Local y Global. El software de gestión de control de acceso deberá contar con formatos de tarjetas preconstituidos dentro de la plataforma y para ser utilizados bastará la escogencia de la casilla correspondiente para tal fin, no deberá existir la necesidad de crear estos formatos desde cero en el software, deberá contar entre otros con formatos de 35, 37, 48 y 50 Bits preconstituidos de esta manera. El software de gestión de control de acceso deberá contar con la opción de visualización de las fotografías de los usuarios del sistema en tiempo real por medio de pop up automático de ser necesario al momento del paso de la tarjeta por el sistema de lectura.  El oferente deberá entregar carta no mayor a 30 días del fabricante de control de acceso ofertado, donde el fabricante avale al oferente para Comercializar, Instalar, Mantener y Soportar la línea de negocios ofertada del fabricante en cuestión. (No distribuidor o canal directo del fabricante) dirigida al proceso y firmada por el representante de la región Colombia o superior del fabricante de control de acceso a ofertar. |  |  |
| **Módulo de Control de Visitantes** | El software de gestión de control de acceso debe contar con una solución de visitantes mono marca en forma de modulo y/o licenciamiento del software de gestión de control de acceso que sea concebida de esta manera para que pueda operar de manera nativa dentro de la misma plataforma, actualizando de manera automática los controladores también del mismo fabricante para la gestión de ingresos de los visitantes del lugar. Evitando así la demora en actualización de usuarios propia de sistemas no nativos o de terceros.  La solución de visitantes debe ser compatible con la lectura del ID completo de la cedula colombiana contenida dentro del código 2D de la misma, realizando esta lectura por medio de un lector 2D el software deberá cargar automáticamente datos de cedula, nombre y apellido del visitante a ingresar en la entidad.  La solución de visitantes debe permitir al visitante por ingresar recibir una tarjeta que estará habilitada para ingresar a las áreas a donde ha sido asignado realizar la visita solamente, prohibiéndosele el acceso a las áreas no autorizadas como corresponde. No se admitirán soluciones de software de visitantes que utilicen la huella como mecanismo de autenticación de los visitantes.  La solución de visitantes debe permitir la carga de descripción de los activos que traiga consigo los visitantes, portátiles, cargadores, teléfonos celulares y demás elementos.  La solución de visitantes debe permitir indicar mediante un cuadro de búsqueda a la persona a la cual el visitante realiza la respectiva visita.  La solución de visitantes debe visualizar cuando fue la última visita del visitante en cuestión.  La solución de visitantes debe estar en la capacidad de tomar una fotografía utilizando una cámara web al visitante en cuestión.  La solución de visitantes debe recibir la siguiente información del visitante: Teléfono, Email, Dirección de residencia entre otros. |  |  |
|
|
| **Controlador Maestro de Acceso** | El Controlador Maestro de Acceso deberá ser tipo montaje pared que no requiera gabinete para ser instalado, cubierta de aluminio o similar, no PCB (Protoboard Circuit Board) con entradas o conexiones mínima para 2 lectoras por medio de conexión OSDP.  El Controlador Maestro de Acceso deberá poseer arquitectura modular, puerto de red Ethernet 10/100 PoE con estándar IEEE 802.3at. El Controlador Maestro de Acceso deberá poder crecer hasta por lo menos 30 lectoras por red local de controladores. El Controlador Maestro de Acceso deberá contar con al menos 1 puerto de comunicación tipo RS485. |  |  |
| El Controlador Maestro de Acceso deberá poder enrolar hasta 50.000 tarjetas y poseer memoria para históricos en desconexión de al menos 30.000 en caso de pérdida de conexión con el Software de gestión de control de acceso. El Controlador Maestro de Acceso deberá proporcionar datos reales en los eventos enviados hacia la base de datos una vez sea restablecida la comunicación con el software de gestión de control de acceso. El controlador Maestro de Acceso deberá permitir la utilización de reglas del sistema en las que al pasar un número determinado de veces la tarjeta por uno de sus lectores, una zona determinada del sistema quede con acceso limitado o nivel de mayor o alta seguridad hasta tanto no se desactive esta función de la misma manera. |  |  |
| El Controlador Maestro de Acceso deberá manejar un mínimo de 5 formatos concurrentes por controlador, salidas tipo relay programables y deberá contar con fuente reguladora de voltaje que de ser requerido tome de manera automática la energía de una fuente de corriente directa, alterna a la alimentación convencional de corriente alterna.  El Controlador Maestro de Acceso deberá permitir la utilización de formatos de tarjeta de 48 Bits o superior.  El Controlador Maestro de Acceso podrá ser alimentado vía PoE y al mismo tiempo recibir suministro eléctrico de una fuente regulada externa interconectada a él, esto con el fin de tener una redundancia de alimentación en el mismo. El controlador deberá estar en la capacidad de realizar carga de la batería con tener conectado la alimentación vía PoE + |  |  |
| El Controlador Maestro de Acceso deberá contar con protección térmica embebida en Alimentación de Entrada, Salida y en la Alimentación hacia las Lectoras.  El Controlador Maestro de Acceso luego de ser configurado de manera inicial deberá́ poder operar de forma Stand Alone sin intervención alguna del software de gestión de control de acceso u otro sistema alterno, siempre de manera local para evitar fallas en su funcionamiento si el servidor por cualquier motivo pierde conexión con el Controlador.  El Controlador Maestro de Acceso deberá poseer por lo menos poseer 4 diferentes leds en total para la visualización de estado y funcionamiento. Y por lo menos dos leds de diferente color para visualización de operación de transmisión y recepción (conectividad con el software de gestión de control de acceso). El Controlador Maestro de Acceso deberá de manera local de ser necesario operar la misma cantidad mínima de lectoras por modulo controlador en configuración puerta esclusa local. |  |  |
| El Controlador Maestro de Acceso deberá poder utilizar para su comunicación Serial y Wiegand u OSDP y el cable tipo AWG 20 - 22, trenzado y blindado. Esto debe estar indicado en la hoja de datos del equipo proveniente directamente del fabricante. El Controlador Maestro de Acceso, en caso de perder alimentación vía suministro eléctrico de una fuente regulada externa interconectada a él, de manera simultánea deberá tomar para si de manera automática un respaldo de energía de Batería externa utilizando una conexión de Batería directa y embebida a él mismo y sin intermediación alguna de una fuente de alimentación externa que cuente con una Batería de respaldo para sí misma. El Controlador Maestro de Acceso deberá permitir la utilización de formatos de tarjeta de 48 Bits o superior.  El Controlador Maestro de Acceso deberá poder comunicar por medio de sus puertos RS-485 a una distancia máxima de 1200 metros y por medio de sus puertos Weigand a una distancia máxima de 150 metros. Esto debe estar indicado en la hoja de datos del equipo proveniente directamente del fabricante.  El controlador Maestro deberá contar con por lo menos una salida TTL adicional, diferente a la utilizada para liberar el sistema del torniquete / Electroimán o puerta de Minusválidos, para ser utilizada en cualquier integración que se requiera a futuro con otro sistema existente en la entidad. |  |  |
| **Servidor** | El software de gestión de control de acceso debe poder operar mínimamente con Servidores de las siguientes características:  Memoria RAM de (8) GB. Procesador Intel Core i5 (Mínimo). Disco Duro de 1TB.  Espacio mínimo libre en Disco Duro (10 GB Instalación y 100 GB para funcionamiento).  Esto debido a la necesidad de garantizar la operación liviana del software en servidores más robustos, se debe garantizar este funcionamiento con carta expedida por el fabricante de los sistemas de control de acceso ofertados (No se admitirán cartas de Canales distribuidores o canales integradores de la o las soluciones ofertadas).  Se solicita que los oferentes oferten mínimamente: |  |  |
| **UPS** | Capacidad de 3 KVA de marca APC, con soportes para instalar en rack y soporte de tres (3) años |  |  |
| **Rack** | ▪Paneles laterales y puerta posterior completamente desmontables |  |  |
| ▪Cierre de seguridad |  |  |
| ▪Paneles de montaje deslizables. Ranuras de acceso de cables desde el panel superior o base del gabinete |  |  |
| ▪Cable Equipotencial |  |  |
| ▪Incluir PDU tipo horizontal, de acuerdo a la cantidad de equipos alimentar y con un crecimiento de al menos del 50%. |  |  |
| ▪Barraje a tierra |  |  |
| ▪40 Unidades de rack, tener en cuenta que tenga el dimensionamiento para alojar el servidor propuesto. |  |  |
|  |  |  |
| **Torniquete**  **Bidireccional tipo gabinete con brazo abatible en acero inoxidable** | |  |  | | --- | --- | | Resistencia del material | Choques, vibraciones, elementos ácidos y alcalinos | | Material tapa | Acero Inoxidable. AISI 304 cepillado espesor 1.5 mm con esquinas frontales entalladas a 45º, de apertura longitudinal autosostenida apoyada con un pistón a gas para evitar su caída | | Apertura del equipo | Apertura longitudinal de la tapa superior autosostenida y soportada con un pistón a gas. | | Material Gabinete | Acero Inoxidable. AISI 304 cepillado espesor 1.5 mm, esquinas redondeadas con radio de 18 mm | | Material Cabezal | Acero carbono pintado con pintura epoxi en polvo con acabado en acero inoxidable | | Material Brazos | Acero Inoxidable. AISI 304 cepillado con tapas protectoras en material plástico. Núcleo interno en acero para mayor resistencia, roscado en el cabezal y fijado con tornillo de difícil acceso | | Tipo de mecanismo | Mecanismo tipo Tiger, bidireccional configurado por software con módulo de control **PWAC** | | Material mecanismo | Partes del mecanismo son construidas en acero al carbono, sin piezas plásticas, con tratamiento de dureza y bicromatizado, proporcionando una mayor resistencia al desgaste y a la corrosión | | Liberación del paso | Liberación de paso por contacto seco o tensión | | Antirretorno | Dispositivo antirretorno, en acero con tratamiento de dureza, con capacidad para torques pesados hasta 2000 N. | | Display | Pantalla intuitiva con pictograma tricolor de última generación (azul, verde y rojo). | | Funcionalidad | Electromecánico para el control de paso en los dos sentidos | | Consumo máximo | 60 W | | Índice de protección | IP53 | | MCBF (Media de ciclos entre fallos) | 1 millón de ciclos | | MTEF (Media de tiempo entre fallos) | 20.000 horas | | MTTR (Media de tiempo para reparación) | Máx. 30 min. | | Temperatura de trabajo | -5 °C a 50°C | | Humedad relativa | Máx. 95% sin condensación | | Peso aproximado | 60 kg. | | Dimensiones (mm) | Alto Gabinete 986 Ancho Gabinete 230 Largo Gabinete1100, Largb bo brazo 474 | | Alimentación | Conmutada “Fullrange” 110 / 220 VAC a través de un totalizador (breaker) | | Garantía | Mínimo 3 año | | Emergencia | Brazo abatible accionado por un electo-iman, con caída automática en caso de falla de energía, | | Monitoreo | Sistema del monitoreo del paso a través de sensores inductivos sin contacto mecánico (vida útil aproximada de 5 millones de ciclos) | | Bloqueo | Bloqueo del giro por el sistema de traba a través de dos triques y dos solenoides normalmente des energizados en estado de stand by | | Amortiguación | Sistema de amortiguación de giro con desacelerador lineal que ofrece mayor confort en el paso y mayor durabilidad del equipo | | Capacidad | Soporta bloqueo de una persona de 120 Kg a 5 km/h | | Mantenimiento | Acceso al mecanismo con llave única y retirada de este por la parte superior del bloqueo para facilitar mantenimiento. Todas las piezas son intercambiables, que facilitan los mantenimientos preventivos y correctivos futuros. | | Protección | Protección contra la entrada de agua, polvo y líquidos corrosivos mediante una vedación | | Accesorios | Accesorios de instalación | | Integración incluida | Base en acrílico para fácil e intuitiva integración de lectores de proximidad | | Recolector de tarjetas | Posibilidad de integración futura de forma modular para recolector de tarjetas | | Instalación | Debe incluir plantilla para facilitar la instalación del equipo en tamaño real | | Servicio posventa | Atención de servicio postventa local directamente de fábrica | | Disponibilidad de piezas | Certificado de fábrica de disponibilidad de piezas hasta por 10 años, luego de descontinuado el modelo | |  |  |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
| **Puerta PMR** | |  |  | | --- | --- | | Material tapa | Acero Inox. AISI 304 cepillado | | Material Pedestal | Acero Inox AISI 304 cepillado con puerta y tapa frontal de carbono, pintados con tinta epoxi en polvo | | Material Pantalla | Acrílico transparente 5 mm con etiqueta con símbolo doble cara | | Material Brazos | Brazo bidireccional en Acero Inox AISI 304 cepillado con desplazamiento en un ángulo de 90º. Compuesto por placa de acrílico con espesura de 5 mm y adhesivo con el símbolo de acceso para discapacitado físico. | | Tipo de mecanismo | Mecanismo bidireccional configurado por software con módulo de control **PWAC** | | Funcionalidad | Electromecánico para el control de paso en los dos sentidos | | Consumo máximo | 60 W | | Índice de protección | IP42 | | MCEF (Media de ciclos entre fallos) | 1 millón de ciclos | | MTEF (Media de tiempo entre fallos): | 20.000 horas | | MTTR (Media de tiempo para reparación) | Máx. 30 min. | | Temperatura de trabajo | 0 °C a 50°C | | Humedad relativa | Máx. 95% sin condensación | | Peso aproximado | 35 kg. | | Dimensiones | Alto x ancho x profundo: 1025 x 1074 x 238 | | Alimentación | Conmutada “Fullrange” (110/220V) | | Garantía | Mínimo 1 año | | Emergencias | En los casos de interrupción de energía o eventos de emergencia, el equipo fue desarrollado para queda libre en ambos sentidos, volviendo a su funcionamiento normal después del restablecimiento de la energía interrumpida | | Ergonomía | Brazo bidireccional, construido en acero inox, que permite el paso de 0,9 metros (espacio suficiente para una silla de ruedas) y desplazamiento en un ángulo de 90º | | Amortiguación | Sistema de amortiguación de giro que ofrece mayor confort en el paso y mayor durabilidad del equipo | | Display | Pantalla intuitiva con pictograma tricolor de última generación | | Seguridad con llave | Puerta provista con cerrojo de seguridad con llave, eso facilita la entrada a la electrónica, así como la fijación del equipo en el suelo, durante su instalación. | | Mecanismo | Mecanismo giratorio con eje central en acero aleado, resistente a la tracción y torsión. Sus componentes son bicromatizados y las piezas reciben tratamiento de dureza y grasa especial, de larga permanencia y durabilidad. | | Display | Pantalla intuitiva con pictograma tricolor de última generación | | Bloqueo | El control de la operación del equipo es realizado por un mecanismo electromecánico localizado en la parte superior del pedestal. Su bloqueo es automático después del retorno del brazo a la posición original. | | Integración incluida | Base en acrílico para fácil e intuitiva integración de lectores de proximidad | | Recolector de tarjetas | Posibilidad de integración futura de forma modular para recolector de tarjetas | | Servicio posventa | Atención de servicio postventa local directamente de fábrica | | Disponibilidad de piezas | Certificado de fábrica de disponibilidad de piezas hasta por 10 años, luego de descontinuado el modelo | |  |  |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
| **Lectoras de proximidad** | El lector deberá estar diseñado para uso con tarjetas tipo sin contacto, material resistente, montaje vertical u horizontal en interiores y en exteriores. El lector deberá contar con certificación Internal Protection mínima IP67 y un bajo consumo de energía. |  |  |
| El lector deberá incluir garantía mínima de 5 años. El lector deberá operar a una frecuencia de 13.56 Mhz con formato de tarjeta de 48 Bits o Superior obligatorio.  El lector deberá incluir puerto de comunicación OSDP Versión 1 o Versión 2, compatible 100% con los controladores de acceso ofertados. |  |  |
| El lector deberá contar con led indicador de actividad, rango de temperatura de operación de mínima de 0 a 65 grados centígrados.  El lector deberá operar con un voltaje de alimentación de 9 a 15 VDC, y contar con certificaciones CE y FCC. |  |  |
| El lector deberá operar dependiendo de un controlador maestro de acceso, pero sin intervención alguna del Servidor u otro sistema alterno, siempre de manera local entre estos. |  |  |
| **Tarjeta de Aproximación** | Las tarjetas deberán ser tipo Mifare - 13.56 Mhz - sin contacto, formato de bits controlado directamente por el fabricante igual o superior a 48 Bits obligatorio. |  |  |
| Las tarjetas deberán ser tipo Imprimibles y contar con mínimo 2KB interno. |
| Las tarjetas deberán cumplir con el estándar CR-80. |
| Las tarjetas deberán cumplir con el formato ISO / IEC 14443. |
| **Cámara Para Registro** | Las cámaras web para la toma de registro fotográfico de visitantes deberán ser compatibles con el sistema operativo instalado en las estaciones de visitantes.  Las cámaras web deberán contar con al menos 1 puerto de comunicación tipo USB para ser interconectadas directamente a las estaciones de visitantes. |  |  |
|
| **Carga de tarjetas al sistema.** | El sistema debe estar en la capacidad de realizar carga masiva de tarjeta habientes desde una base de datos otorgada por la institución, ya sea en Excel o similar para facilidad del inicio de operación del sistema y posterior edición por demanda. |  |  |
| **Lector de código de barras 2D** | Las Lectoras 2D deberán permitir la lectura del ID completo contenido dentro de la cedula colombiana.  Las lectoras 2D deberán contar con al menos 1 puerto de comunicación tipo USB para ser interconectadas directamente a las estaciones de visitantes.  Las lectoras 2D deberán cargar de manera automática hacia el módulo de visitantes los datos de por lo menos primer nombre, primer apellido y número de cédula al momento de realizar la lectura del código 2D establecido en la cédula colombiana. |  |  |