
 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">1 de 37</p>

ANEXO TÉCNICO


ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.

Sptiembre de 2019

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">2 de 37</p>


Contenido

1. GLOSARIO.....	3
2. OBJETO.....	4
3. ALCANCE.....	4
4. ENTREGABLES.	4
5. GARANTÍA.	5
6. COMPONENTES DEL PROCESO.....	6
6.1. Componentes del sistema.....	6

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p>SENADO DE LA REPÚBLICA</p>	3 de 37

1. GLOSARIO.

- **ANS:** Acuerdo de Niveles de Servicio o *Service Level Agreement* (SLA)
- **CHECKLIST:** Lista de chequeo
- **INFRAESTRUCTURA:** Son los recursos de tecnología compartidos que proporcionan la plataforma para alojar las aplicaciones de sistemas de información específicas del Senado de la República, incluye hardware, software y servicios que se comparten a través de todas las unidades de la empresa. La infraestructura de TI proporciona los fundamentos para ofrecer servicios a clientes externos, manejar los procesos de negocio
- **OFERENTE:** Persona natural o jurídica interesada en ofrecer la prestación o suministro de los bienes o servicios objeto del presente PLIEGO y que se encuentra habilitado para presentarse como OFERENTE de EL CLIENTE de acuerdo con los parámetros que éste ha establecido.
- **PROYECTOS ESPECIALES:** Se consideran proyectos especiales aquellos derivados de implementaciones de software, nuevas aplicaciones o traslados masivos de usuarios por adecuaciones físicas o apertura de nuevas oficinas.
- **PLIEGO (Request For Proposal o Solicitud de Cotización):** Nombre que recibirá el documento que será enviado al OFERENTE invitándolo a ofrecer.
- **TI:** Tecnologías de información.
- **Sistema de Control de Accesos:** Un sistema de control de acceso es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura (clave por teclado, tags de proximidad o biometría) y a su vez controlando el recurso (puerta, torniquete o talanquera vehicular) por medio de un dispositivo eléctrico como un electroimán, cantonera, pestillo o motor.
- **Sistemas de CCTV:** “Circuito Cerrado de Televisión” Sistema que permite visualizar diferentes sitios de una edificación con el objetivo de incrementar el nivel de seguridad y tener medios probatorios en caso de algún incidente de seguridad. Este Sistema está compuesto por cámaras de video, servidores de grabación y clientes de reproducción y visualización.
- **Sistema de Detección de Incendios:** Este Sistema permite detectar una condición de alarma temprana ocasionada por un incendio, su misión principal a diferencia de los sistemas de intrusión es Salvar vidas por encima de la protección de los bienes. Este Sistema está compuesto por Detectores, Estaciones manuales, sirenas, central de incendio, entre otros.
- **Sistema de Control de Visitantes:** Este Sistema está orientado a solucionar la problemática de mantener un adecuado registro y control de todas las personas que a diario ingresan a las instalaciones de una compañía, bien sean visitantes frecuentes o visitantes ocasionales, todo ello sin incurrir en trámites manuales o papeleo por parte de los porteros o recepcionistas o de las personas que reciben la visita.
- **VMS:** “Video Management System” Es un sistema que se utiliza para visualizar y administrar video en vivo y grabado desde dispositivos IP y/o analógicos conectados a un sistema de CCTV.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	4 de 37

2. OBJETO.

El presente documento describe los requerimientos y especificaciones técnicas mínimas para el desarrollo de un proyecto de seguridad para una edificación con la implementación de un sistema de Control de Acceso peatonal y vehicular, integración de sistemas de Circuito Cerrado de Televisión, integración de sistemas de visitantes e Integración de sistemas de detección de incendio, con su administración, supervisión e integración (unificación) de diferentes subsistemas bajo una única plataforma de gestión de eventos.

3. ALCANCE.

Reposición y cambio de todos los controles de acceso, carnetización de todos los funcionarios, registro de visitantes e ingreso de vehículos al Senado de la República, integración del circuito cerrado de televisión mediante el software de gestión propuesto, integración del sistema contra incendios del edificio e integración con la plataforma Welcome de autenticación.

El sistema deberá ser de naturaleza modular y permitir la expansión en lo referente a capacidad y funcionalidad, mediante la adición de sensores, dispositivos de entrada y salida, paneles controladores autónomos y estaciones de trabajo o clientes móviles.

Los equipos suministrados deberán tener respaldo de fábrica para suministrar repuestos, soporte técnico y actualización de software por un periodo no inferior a 5 años, los costos ya deben estar incluidos.

El suministro ofrecido deberá incluir todos los equipos y accesorios que sean necesarios, así no se encuentren descritos en estas especificaciones, para garantizar el correcto funcionamiento de cada subsistema de acuerdo a lo especificado, adicionalmente se deben incluir las pruebas, capacitación, entrenamiento que sean necesarios para la correcta operación y mantenimiento de los diferentes sistemas.

4. ENTREGABLES.


Los entregables de las actividades realizadas estarán reflejados en todas las tareas y acciones que desarrolle el proponente; los entregables deben cumplir las siguientes características:

El sistema de control de acceso comprende identificación y toma de decisiones para garantizar ingreso del personal a zonas restringidas creando un entorno más seguro al Senado.

El sistema deberá operar en una arquitectura cliente/servidor bajo el sistema operativo Microsoft Windows Server vigentes mínimo 2016 y gestionar los datos mediante bases de datos Microsoft SQL server mínimo 2016 para garantizar el soporte en los próximos 5 años.

El sistema deberá estar en la posibilidad de operar bajo tecnología de 64 bits garantizando el máximo aprovechamiento de los recursos de hardware disponibles en el mercado.

Las estaciones de trabajo del sistema (clientes) deben ser fáciles de usar, emplean menús basados en iconos y la creación de mapas o gráficos en color. La interfaz de usuario será

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p>SENADO DE LA REPÚBLICA</p>	5 de 37

personalizable, capaz de ofrecer una apariencia única acorde a los privilegios del usuario autorizado en el sistema.

El sistema deberá estar en la capacidad de aceptar diferentes tipos de formatos de imágenes rasterizadas (mapas de bits):

- Formato de imagen JPEG / JPG
- La extensión de imagen .gif
- Formato de imagen PNG
- La extensión de imagen .tiff / .tif
- El formato de imagen RAW
- El formato de imagen BMP
- La extensión de archivo de imagen .psd
- La extensión de dibujo .dwg

De esta manera personalizar la interface de usuario para su fácil administración y manejo.

Deben contar con la posibilidad de manejar entorno vía web y aplicación para dispositivos móviles sencillo y práctico para el usuario final, proporcionando la portabilidad que el cliente requiera y disponibilidad en todo momento.

El sistema de control de accesos deberá contar con las funcionalidades tales como monitoreo de eventos, administración de personal, vistas dinámicas, tareas programadas como *backups* automáticos, reportes personalizados, entre otras.

OBJETIVOS


- Aumentar el nivel de seguridad de la edificación al supervisar y controlar las áreas a las cuales una persona pueda ingresar.
- Proveer reportes sobre los movimientos de los empleados y del personal visitante.
- Gestionar el control de puertas mediante detectores de apertura, botones pulsadores, electroimanes y lectoras de tarjetas o biometría.
- Detección de tránsito de personas en horarios y zonas especificadas en los que no deberá haber ningún tipo de circulación peatonal y/o vehicular.

5. GARANTÍA.

Se deberá garantizar el perfecto funcionamiento, compatibilidad y sincronización de cada uno de los elementos suministrados e instalados durante la ejecución de las actividades.

El proveedor deberá garantizar para las actividades de personal en las cantidades y calidades requeridas.

El proveedor deberá garantizar los repuestos en las cantidades y calidades requeridas y en los tiempos estipulados. Los repuestos deberán ser nuevos, no remanufacturado ni usados.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	6 de 37

Para el stock de equipos deberá garantizar el perfecto funcionamiento, compatibilidad y sincronización de cada uno de los elementos suministrados e instalados. Garantía de funcionamiento, de daños y defectos de fabricación por tres años.

De presentarse alguna falla o mal funcionamiento en los repuestos o en el stock de los equipos, el proveedor estará en la obligación de darle solución al mal funcionamiento, a la falla o al daño reportado y suministrar el elemento a cambiar de ser necesario y el cambio del equipo si se requiere.

Para el caso de los mantenimientos de presentarse alguna falla en los equipos intervenidos deberá darle solución al mal funcionamiento a la falla o al daño reportado y garantizar las condiciones de operación del equipo.

6. COMPONENTES DEL PROCESO.

6.1. Componentes del sistema.

El Senado de la República requiere que se ejecuten las actividades necesarias para la realización de la correcta administración, gestión, operación, actualización y monitoreo de los servicios de control de acceso de funcionarios, visitantes y de vehículos que soportan la operación de la entidad. A partir de lo indicado se establecen los requerimientos técnicos para los servicios actuales de la entidad.


SOFTWARE DE CONTROL DE ACCESO

El software de control de acceso deberá permitir la escalabilidad y crecimiento a futuro dando un máximo de disponibilidad en cuanto a ampliación de negocio.

Las características mínimas en simultáneo del software deben ser:

- Número de lectoras en línea mínimo 125.
- Número de entradas en línea 4800.
- Número de salidas en línea 4900.
- Número de registros de personal tarjetahabiente 44000.
- Número de clientes simultáneos incluidos / expandible mínimo 20/255.
- Número de clientes de carnetización Incluidos / expandible mínimo 2/255.

El Software debe permitir agregar clientes de monitoreo y administración del sistema y clientes de creación de credenciales adicionales a una licencia del sistema. Las conexiones cliente simultáneas deben ser tabuladas por la conexión de cliente web/móvil, monitoreo de alarma y administración del software. El software está diseñado para en caso de ser requerido una expansión manejar por servidor no menos de 5000 lectoras y 500000 tarjetahabientes.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p>SENADO DE LA REPÚBLICA</p>	7 de 37

INTERFAZ DE OPERADOR DE ADMINISTRACIÓN


El sistema de control de accesos deberá emplear una interfaz de operador de administración para controlar lo siguiente:

- Hardware (lectores, entradas, salidas, sistemas de vídeo, controles de puertas, CCTV y otros sistemas integrados).
- Configuración de los registros de personal, los operadores y los privilegios de operador.
- Mapas gráficos.
- Diseños de aplicación.
- Vistas dinámicas.
- Consultas.
- Importación o exportación de objetos, incluidas imágenes.
- Variables del sistema.
- Informes (periódicos u ocasionales).
- Funciones del sistema (comando y control de eventos, acciones, programas).
- Visualización de una lista de objetos en una cuadrícula, cuyos valores se puedan modificar y permitan responder a cambios de estado en tiempo real.
- Programación de copias de seguridad.
- Supervisión de la configuración y el rendimiento del sistema.
- Diseño e impresión de carnets.
- La interfaz gráfica de usuario deberá poder ser configurada por el administrador del sistema para controlar las vistas y el acceso a cada operador de la Estación de supervisión.

INTERFAZ DE OPERADOR DE SUPERVISIÓN/SUPERVISIÓN DE ACTIVIDADES

El sistema de control de accesos deberá estar equipado con un componente de supervisión que debe poder entre otras tareas, mostrar el estado actual de cualquier objeto del sistema. Además, la Estación de supervisión deberá poder mostrar un registro de todas las actividades que ocurran en el sistema, desde cambios en el estado de los objetos a información de control de acceso. Todo el texto de los eventos (alarmas) del sistema se deberá poder configurar para que se muestre en color según la prioridad del evento especificada por el usuario.

La Estación de supervisión deberá poder mostrar todos los cambios que ocurran en un objeto sin necesidad de que los mensajes de actividad asociados al objeto se enruten a dicha estación. El operador deberá disponer de los permisos adecuados para ver y/o controlar los objetos del sistema de control de accesos.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	8 de 37

Los usuarios deberán poder personalizar la interfaz de la estación de supervisión. El sistema de control de accesos deberá permitir que el usuario final cree un diseño de aplicación personalizado para la estación de supervisión. La estación de supervisión deberá admitir varios diseños de aplicación que se debe poder asignar a los operadores. Cada diseño de aplicación puede tener varios paneles en la misma ventana. Los paneles, a su vez, pueden tener varias fichas de forma que se pueden mostrar diferentes objetos, tales como cámaras y rondas, en el mismo panel. Los paneles deberán poder contener: actividad general, actividad de evento (alarma), información de pase de tarjeta dinámica, cámaras de vídeo y rondas, mapas, vistas dinámicas, informes y enlaces a aplicaciones externas. Cada panel debe poder moverse a una pantalla concreta.

El sistema de control de accesos deberá ofrecer las siguientes capacidades funcionales al operador de supervisión:

Deberá proporcionar una lista con desplazamiento de las líneas o títulos que muestren la actividad actual en el sistema.

Deberá mostrar la actividad en tiempo real a medida que el hardware de campo transmita los datos.

Deberá incluir iconos que indiquen el tipo de actividad y una descripción textual de esta.

El color de los marcos de los mosaicos, iconos y/o el texto deberá indicar el tipo o la importancia de la información que contienen.

Una serie de menús, organizados de forma desplegable o en árboles, permitir a la estación de supervisión la realización de acciones manuales, como “desbloqueo momentáneo de puerta” para una determinada puerta.


Como parte de la capacidad de acción manual, el sistema deberá ofrecer pantallas o cuadros en los que se consulte al operador sobre aspectos específicos, tales como la hora de inicio y fin, y sirvan de guía para la realización de acciones manuales.

Una interfaz gráfica de usuario que muestre las imágenes del personal al entrar, así como las imágenes del personal almacenadas disponibles en el sistema de control de accesos.

Capacidad para ver una lista clasificable de las alarmas o los eventos activos y de las alarmas que han estado activas recientemente o la actividad reciente.

Capacidad para ver vídeo del sistema VMS en la misma interfaz gráfica de usuario. La interfaz gráfica de usuario de la pantalla de vídeo deberá poder mostrar varios paneles de vídeo en directo o grabado y debe incluir controles de cámara en pantalla para cada ventana en directo, con lo que pueda ofrecer control de las cámaras individuales.

De entregar una interfaz gráfica de usuario que minimice el número de clic en el mouse o pulsaciones de teclado del operador.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	9 de 37

Entre los controles del mouse se debe incluir elementos emergentes mediante el botón derecho del mouse y selecciones predeterminadas resaltadas.

Los objetos se deberán mostrar al operador según el privilegio de operador que se tenga asignado. El operador solo debe poder supervisar o controlar los objetos para los cuales tenga privilegios asignados.

Cuando un operador cierra sesión en una estación de trabajo y otro inicia sesión, los objetos de la pantalla de la estación de trabajo se deberán actualizar dinámicamente para mostrar únicamente aquellos para los que el nuevo operador dispone de privilegios.

Permitir la personalización de las columnas tal como se definen por el privilegio del operador, entre lo que se debe incluir:

- Ajustar el ancho (sobre la marcha o mediante programación previa).
- No mostrar las columnas (sobre la marcha o mediante programación previa).
- Ordenar las columnas seleccionadas (para seguir las convenciones estándares de Windows).

Permitir una función de “congelación” de imagen. Incluir una función de “congelación de tiempo de espera” configurable que permita seleccionar una actividad y evite temporalmente la visualización de las actividades posteriores con las que se finaliza la visualización de la actividad seleccionada en la pantalla. Un evento de interrupción debe deshabilitar la función de congelación.

Admitir varios paneles para la visualización de eventos, actividades, vídeo, imágenes de personal y mapas.


Mostrar el número de motivos activos de un evento.

Permitir adjuntar un mensaje de registro a un evento, incluso después de que el evento se haya reconocido.

Ofrecer la capacidad de adjuntar mensajes de registro predefinidos a un evento tras el reconocimiento.

CONFIGURACIÓN DEL SOFTWARE

Las herramientas de configuración del sistema de control de accesos deberán utilizar controles de configuración inteligentes. El sistema debe estar estructurado de forma que el operador no pueda usar funciones de configuración que no sean válidas para la configuración utilizada. El sistema deberá permitir realizar búsquedas en las listas del explorador mediante operadores de filtrado tales como “comienza por”, “termina en”, “contiene”, entre otras. El sistema también deberá permitir al operador realizar búsquedas con operadores de filtrado en cualquier clase de objeto del sistema en la aplicación de administración y de la estación de supervisión.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	10 de 37

El sistema de control de accesos deberá permitir las descripciones de texto de todos los objetos configurados. El sistema de control de accesos deberá permitir el cambio de nombre de una descripción de título existente sin necesidad de eliminar los subcomponentes de dicho objeto de configuración. El sistema de control de accesos deberá eliminar automáticamente del sistema todas las referencias de configuración a un objeto que se ha eliminado. El sistema de control de accesos proporcionará automáticamente nombres predeterminados para todas las entradas, salidas, lectores y tarjetas de extensión. El sistema de control de accesos debe mostrar con claridad qué objetos de hardware (entradas, salidas, lectores) de un controlador se han configurado y cuáles no.

El sistema de control de accesos permitir la configuración de plantillas. Las plantillas de objetos compatibles deberán poder ser configuradas por el operador para proporcionar valores predeterminados a los campos de datos en una configuración de clase de objeto.

El sistema de control de accesos deberá admitir múltiples grupos para cualquier tipo de objeto. En general, se debe poder usar un grupo siempre que se haga referencia a un objeto individual en el sistema de control de accesos. Por ejemplo, se puede usar un grupo en lugar de un objeto al configurar una par programación/objeto en una autorización o al configurar una acción manual para desbloquear una puerta.

El sistema de control de accesos deberá permitir generalmente que se agrupe cualquier objeto del sistema, incluidos el personal, las puertas, las entradas y las autorizaciones.


El sistema de control de accesos deberá restringir la visualización y el control de objetos en las estaciones de administración y supervisión mediante privilegios de operador. El sistema de control de accesos deberá admitir la configuración de restricciones de operador según las clases de objetos o para cada objeto individual. El sistema de control de accesos debe mantener una distinción entre los objetos que se estén supervisando y los que se estén controlando, impidiendo a los operadores que realicen acciones manuales en objetos para los que no disponen de privilegios de acciones manuales. Deberán existir diferentes niveles de controles en el sistema para los privilegios de administración frente a los de supervisión.

El sistema de control de accesos deberá admitir múltiples cuentas de operador múltiples niveles de privilegios definibles por el usuario.

El sistema de control de accesos deberá permitir la configuración de los controladores mediante una navegación jerárquica basada en árbol y unos menús contextuales.

El sistema de control de accesos deberá permitir a los controladores descargar actualizaciones de firmware.

El sistema de control de accesos deberá admitir el inicio de sesión único de Windows (SSO) que integra las credenciales de inicio de sesión con los permisos del operador para proporcionar una autenticación y autorización de usuario totalmente integradas.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	11 de 37

El sistema de control de accesos deberá proporcionar un proceso de actualización de cliente automática para una rápida distribución de las actualizaciones de la aplicación.

El sistema de control de accesos deberá contar con una ayuda contextual en línea (en la pantalla) disponible en cualquier punto en que se requiera una entrada de operador.

El sistema de control de accesos debe admitir la capacidad de definir configuraciones de área. Un "área" se define como una región física delimitada por puertas. Un área consistirá en una sala, una o más ubicaciones dentro de un edificio o un edificio entero. Todas las áreas configuradas deberán tener puertas de acceso de entrada/salida, para que no exista ninguna forma de abandonar un área sin presentar una credencial ante un lector o puerta.


El sistema de control de accesos deberá tener la posibilidad de implementar antipassback el cual controlará el acceso en función de la ubicación del portador de tarjeta. El sistema de control de accesos denegará el ingreso o salida a un punto específico a los portadores de tarjeta que hayan infringido las reglas de antipassback. En caso de que un portador de tarjeta abandone un área sin presentar su credencial en el lector/puerta de acceso de salida y posteriormente intente volver a entrar en el área pasando su tarjeta por el lector/puerta de acceso de entrada, se producirá una denegación de acceso. El sistema de control de acceso debe proporcionar la capacidad de excusar a portadores de tarjeta individuales que hayan infringido las reglas de antipassback. La opción de excusar deberá ofrecer asimismo la capacidad de excusar a todos los portadores de tarjeta.

El antipassback debe continuar vigente durante un fallo de las comunicaciones. Los controladores del sistema de control de accesos deben tener la capacidad de ser clústeres en un grupo.

El sistema de control de accesos debe ofrecer restricciones de ocupación para las áreas. Las restricciones se aplicarán a portadores de tarjeta individuales (personal) o a grupos de portadores de tarjeta definidos por el usuario. Las áreas deben ser configurables para ofrecer límites de número mínimo y máximo de personal que puede acceder a un área al mismo tiempo. Debe ser posible activar un evento en función de una infracción a cualquiera de estas reglas. Los eventos serán configurables en función de los siguientes criterios:

- Estado ocupación máxima.
- Estado ocupación mínima.
- Estado ocupación máxima grupo.
- Estado ocupación mínima grupo.
- Recuento de personal (definido por el usuario)
- Estado de infracciones (infracción de antipassback de entrada/salida, entre otras.)

El sistema de control de accesos debe admitir el control de área para ofrecer la capacidad de localización de empleados. Con esta función, un operador debe poder consultar la

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">12 de 37</p>

ubicación actual de los portadores de tarjetas. Se debe poder generar vistas dinámicas e informes que muestren a los portadores de tarjetas específicos presentes en cada área definida.

Los controladores del sistema de control de accesos deberán admitir hasta 1000 autorizaciones por persona.

El sistema de control de accesos deberá admitir la activación de autorizaciones, así como la fecha y hora de expiración

El sistema de control de accesos deberá admitir eventos configurables por el operador, entre los que se incluyan la programación de eventos y el desencadenamiento de eventos basado en la acción.


El sistema de control de accesos deberá ofrecer ocho niveles de prioridad de eventos configurables con un total de 200 prioridades de eventos numeradas. El operador debe poder definir colores y etiquetas personalizados para cada nivel de prioridad individual.

El sistema de control de accesos deberá ofrecer métodos para importar y exportar manualmente los datos seleccionados en formato XML. Este mecanismo debe admitir la importación y exportación de la mayoría de las clases o tipos de datos en el sistema. Se deberán cumplir la validación de datos específicos y los requisitos de inicio de sesión. El sistema también deberá admitir la importación de archivos CSV.

El sistema de control de accesos debe poder conectarse a un origen de servicio de directorio mediante el *Lightweight Directory Application Protocol* (Protocolo de Aplicación Ligera de Directorio, LDAP). La conexión al origen de LDAP debe poder configurar el usuario directamente desde el sistema de control de accesos y no requerir código personalizado. La interfaz LDAP también permitir la asignación automática de autorizaciones del sistema de control de accesos basadas en datos del registro de LDAP. Esta característica debe estar disponible mediante la adición de licencia.

El sistema de control de accesos deberá proporcionar informes de datos configurables y personalizados para la configuración de la base de datos, la actividad histórica (Registro) y el seguimiento de auditoría. Los informes predefinidos deberán estar disponibles para su descarga y para importarlos en el sistema. Los informes se deben poder exportar en formatos como PDF, RTF, TXT, TIFF, y Excel (XLS).

El sistema de control de accesos deberá facilitar un motor de consulta que resultará de gran utilidad para los usuarios sin ningún conocimiento de SQL o cualquier otro lenguaje de consulta específico. Deberá permitir a los usuarios realizar solicitudes frente a los conjuntos de datos con relaciones preconfiguradas entre tablas. Las relaciones reflejarán las relaciones reales entre los objetos de base de datos y el usuario debe poder insertar condiciones en cualquier campo disponible del tipo de objeto seleccionado y sus objetos subordinados.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	13 de 37

El sistema de control de acceso deberá contar con licencia de protocolo de comunicación *Bacnet* para supervisión del sistema de detección de incendios existente en el Senado.


Se deberá incluir el licenciamiento para la integración nativa de los lectores biométricos que permitan enrolamiento desde software cliente de control de acceso.

El sistema debe tener la capacidad para realizar particiones del sistema, es decir, debe poder manejar múltiples áreas o edificios como si fueran independientes compartiendo las mismas licencias y servidor suministrados.

El sistema deberá tener la opción de redundancia en servidor Activo - Activo para continuidad de la operación por medio de licenciamiento adicional, esta opción no se usara en esta etapa del sistema pero se contemplara para futuros proyectos.

Actualmente el Senado cuenta con una solución *Welcome* de gestión de visitantes. El sistema de control de accesos deberá ser compatible con esta solución y contemplar los elementos necesarios a nivel de licenciamiento e ingeniería para esta integración. Una vez implementado e integrado el sistema de control accesos y gestión de visitantes deberá tener las siguientes funcionalidades:

- Integración con lectores biométricos para captura de la huella de los visitantes en los puntos de registro.
- Réplica de huella de visitantes a lectores biométricos conectados en la red para accesos mediante huella digital por los molinetes.
- Integración con sistema de control de acceso para creación de *card holder* con permisos de acceso de acuerdo a los diferentes niveles.
- Borrado automático de huellas de manera masiva al finalizar el día.
- El sistema de visitantes deberá permitir enviar al sistema de control de acceso la información del visitante (Identificación, nombre, apellidos, nivel de acceso, número de tarjeta ID (cédula), para que esta persona quede habilitada y pueda ingresar por medio de su huella.
- El sistema de visitantes deberá replicar las huellas a los dispositivos biométricos conectados en la red y automáticamente esa persona deberá quedar habilitada para poder ingresar por medio de su huella.
- Al finalizar la visita, la persona saldrá por los dispositivos biométricos de salida, el sistema de visitantes deberá ejecutar un evento de salida automática en el sistema de control de acceso con el ID (cédula), el cual deberá dar salida al visitante en el sistema de control de acceso y del sistema de control de visitantes.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p>SENADO DE LA REPÚBLICA</p>	14 de 37

- Al finalizar el día, el sistema de visitantes deberá ejecutar una tarea automática para que borre todas las huellas de los biométricos conectados en la red.

COMPATIBILIDAD DE TARJETAS Y LECTORES

El sistema de control de accesos deberá admitir hasta varios formatos de tarjeta y tipos de lector de tarjeta. El sistema de control de accesos deberá admitir las siguientes funciones para los lectores conectados directamente:

- Formatos de tarjeta definidos por el usuario hasta 256 bits.
- Formatos de tarjetas del sistema de control de accesos 10 por controlador.
- La posibilidad de asignar hasta 10 formatos de tarjeta por lector.
- Compatibilidad con *Wiegand* y teclados de 3x4 matriz.
- La inclusión de plantillas biométricas para tarjetas inteligentes.

El sistema de control de accesos deberá admitir los siguientes tipos de lectores cuya comunicación con el controlador sea mediante el protocolo OSDP encriptado AES 128:

- Lectores multitecnología.
- Lectores de proximidad.
- Lectores biométricos.
- Lectores de tarjetas inteligentes.
- Lectores inalámbricos.

Las características mínimas de software para el sistema de control de acceso deben ser:

- Asignación de plantillas de aplicación a eventos específicos
- Seguimiento eficiente de datos consolidados con reportes de configuración, auditoría y registro diario global
- La administración de la ocupación y el control del área permitan impedir los reingresos, definir las restricciones de ocupación y los procedimientos de cierre en áreas clasificadas y sensibles
- Deberá ser una plataforma abierta, que ofrecer cientos de soluciones integradas de diferentes fábricas, que incluyen vídeo, intrusión, intercomunicación, gestión de alarmas contra incendios, PSIM y más. Las integraciones deben estar altamente probadas y se deben entregar a través de una interfaz intuitiva al operador.
- Autenticación de Windows en dominio y dominio confiable.
- Idiomas soportados: árabe, portugués (Brasil), checo, danés, holandés, inglés, francés, alemán, húngaro, italiano, japonés, coreano, polaco, ruso, chino simplificado, español, sueco, chino tradicional y turco.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">15 de 37</p>

- El software deberá permitir la creación de diferentes perfiles de usuarios; dentro de estos se deberá incluir el perfil de usuario administrador, el perfil de usuario administrador de subsistemas (sin acceso a configuración), el perfil de usuario de lectura, el perfil de usuario de reportes. El sistema deberá llevar registro de todas las acciones de cada uno de los usuarios. Así mismo deberá contar con la capacidad de almacenar un log de eventos con la gestión de cada uno de los usuarios.
- El sistema deberá contar con un despliegue gráfico de los planos de los edificios indicando cada uno de los elementos a controlar o a supervisar con nombres en español y dentro de un entorno espacial acorde a su ubicación.
- El sistema deberá estar en capacidad de soportar comunicación para lectores y biométricos utilizando el Protocolo de Dispositivo Abierto Supervisado (OSDP) encriptado AES128.

REQUERIMIENTOS DE HARDWARE.


Los requerimientos mínimos de hardware para el sistema de control de accesos son los siguientes, teniendo en cuenta que este documento contiene el mínimo y especificación recomendada necesaria para la versión de características mínimas del software de control de accesos, de acuerdo a la capacidad del sistema o si cualquier otro software se va a instalar en la computadora o el ordenador va a estar muy cargado; los requisitos se deben aumentar en consecuencia. Esto también aplica para la base de datos SQL a utilizar de acuerdo a las capacidades del sistema.

REQUISITOS MÍNIMOS DEL SERVIDOR.

- Procesador Intel Xeon E3-1240v5, 3.5 GHz, 4 cores o superior.
- Unidades de disco duro unidades dobles. Dos discos duros 600 GB SAS 15K RPM, RAID 1 o superior.
- Memoria RAM 32 GB 1600 MHz RDIMM o superior.
- Tarjeta adaptadora de red puerto de red de gigabit con mínimo 4 puertos.
- Unidad de DVD recomendada.
- Servidor para montaje en rack.
- Base de datos SQL Server 2016 SE.
- Sistema operativo Windows Server 2016, SE, 64 bit, 5 CALs.

REQUISITOS DE LA ESTACIÓN DE TRABAJO

- Procesador Intel Core i5-6600 3.9 GHz o superior.
- 2 Unidades de disco duro 1 TB o superior.
- Velocidad del disco 7200 rpm o superior en Raid 1.
- Memoria Ram 16 GB DDR4 Mínimo.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p>SENADO DE LA REPÚBLICA</p>	16 de 37

- Tarjeta de red 2 Puertos de red Gigabit.
- Tarjeta de vídeo NVIDIA P600 o superior.
- Sistema operativo Windows 10 Professional.

CONTROLADOR INTELIGENTE

Los controladores del sistema deben ser flexibles en su selección ofreciendo modelos de montaje en pared o en rack; adicionalmente, se deberá contar con modelos para 1, 2, 4, 8, 16 y 32 lectoras. Los controladores inteligentes deben contar con capacidad de trabajo con sistemas de lectores inalámbricos, permitiendo tener instalaciones de tipo híbrido (cableadas e inalámbricas) a lo largo de la edificación.

CONTROLADORES 16 LECTORAS

Las características técnicas de los controladores deben ser:

- Listo para conexión a la red de datos Ethernet mediante 2 puertos de 1 Gbps.
- El controlador deberá poseer una memoria interna con una capacidad mínima de 2 GB.
- El controlador deberá poseer un slot para memoria flash con un mínimo de crecimiento de 16 GB.
- El controlador deberá soportar 500000 usuarios de tarjeta Mínimo.
- Pantalla de estado y diagnóstico.
- Entrada dedicada para interacción con el panel de detección y alarma contra incendio para apertura de puertas bajo condiciones de alarma de fuego.
- Doble tarjeta de red Gigabit y encriptación FIPS 197 y AES 256 bit.
- Las temperaturas de operación aceptables deben estar entre 0 y 50 °C (32 - 122 °F) y con grado de humedad con niveles entre 5 % y 95 % no condensado.
- Deberá poseer pantalla LCD para los mensajes de diagnóstico los mensajes como mínimo deberá indicar información de arranque, fecha y hora, versión de firmware, información de estado, configuración de energía, dirección IP y MAC del controlador, estado de conectividad con el servidor, información de tarjetas y lectoras, información de las entradas y salidas cuando presentan cambio de estado, test de operación del puerto ethernet.
- El controlador como medio de expansión deberá poseer un puerto RS485 para módulos de entradas, módulos de salidas y módulos que permitan la extensión de lectores wiegand a largas distancias.
- Deberá tener la opción de diagnóstico mediante web server.
- El controlador admite varias tarjetas por titular y varios formatos con el fin de conseguir una solución muy segura y flexible.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p style="text-align: center;">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p>Página</p>
	<p style="text-align: center;">SENADO DE LA REPÚBLICA</p>	<p>17 de 37</p>


- El controlador compatible con los formatos ampliados de tarjeta de hasta 256 bits, proporcionando la máxima flexibilidad al configurar formatos de tarjetas personalizados.
- El controlador deberá ser compatible con todo el formato FASC-N de 200 bits que cumple la iniciativa FIPS 201 del Gobierno de los EEUU, así como el formato GUID de 128 bits para las credenciales PIV-I.
- Capacidad para usar varios tipos de tarjeta (como las de 26 bits, 37 bits o Corporate 1000)
- Memoria y respaldo RTC pila de litio CR 2032 para respaldo de RTC; las copias de seguridad de base de datos y transacciones de búfer se almacenan en memoria no volátil.
- Entradas dedicadas: Armario anti manipulación, fallo de CA, batería baja.
- El controlador deberá poder soportar hasta 256 entradas y salidas mediante módulos adicionales.
- El controlador deberá tener la posibilidad de instalación en rack o en muro.
- El controlador deberá tener la posibilidad de conectar los lectores directo mediante protocolo OSDP a las tarjetas de comunicación (al menos 8 lectores por tarjeta de comunicación para un total de 16) o con módulos de expansión por puerta con conexión IP.
- El controlador deberá poder manejar al menos 2 buses de 8 lectoras con comunicación OSDP multi-drop.

Deberá cumplir con las siguientes normatividades:


- Access Control: UL 294, CSA C22.2 No. 205 (Canada); UL 1076, ULc 1076 (Canada)
- CE: EN 55022, EN 55024, EN 60950-1
- Safety: IEC 60950-1
- EMI: FCC Part 15 Class A, EN 55022, ICES-003(Canada), VCCI / Class A ITE (Japan), C-Tick (AS/NZS CISPR 22 - Australia/New Zealand)
- EMC: EN 55024, EN 50130-4, IEC 62599-2, EN 61000-6-1
- Encryption: FIPS 197, FIPS 201

CONTROLADORES 8 LECTORAS.

Las características técnicas de los controladores deben ser:

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	18 de 37

- Listo para conexión a la red de datos Ethernet mediante 2 puertos de 1Gbps.
- El controlador deberá poseer una memoria interna con una capacidad mínima de 2 GB.
- El controlador deberá poseer un slot para memoria flash con un mínimo de crecimiento de 16 GB.
- El controlador deberá soportar 500000 usuarios de tarjeta mínimo.
- Pantalla de estado y diagnóstico.
- Entrada dedicada para interacción con el panel de detección y alarma contra incendio para apertura de puertas bajo condiciones de alarma de fuego.
- Doble tarjeta de red Gigabit y encriptación FIPS 197 y AES 256 bit.
- Las temperaturas de operación aceptables deben estar entre 0 y 50 °C (32 - 122 °F) y con grado de humedad con niveles entre 5 % y 95 % no condensado.
- Deberá poseer pantalla LCD para los mensajes de diagnóstico los mensajes como mínimo deberá indicar información de arranque, fecha y hora, versión de firmware, información de estado, configuración de energía, dirección IP y MAC del controlador, estado de conectividad con el servidor, información de tarjetas y lectoras, información de las entradas y salidas cuando presentan cambio de estado, test de operación del puerto *ethernet*.
- El controlador como medio de expansión deberá poseer un puerto RS485 para módulos de entradas, módulos de salidas y módulos que permitan la extensión de lectores *wiegand* a largas distancias.
- Deberá tener la opción de diagnóstico mediante *web server*.
- El controlador admite varias tarjetas por titular y varios formatos con el fin de conseguir una solución muy segura y flexible.
- El controlador compatible con los formatos ampliados de tarjeta de hasta 256 bits, proporcionando la máxima flexibilidad al configurar formatos de tarjetas personalizados.
- El controlador deberá ser compatible con todo el formato FASC-N de 200 bits que cumple la iniciativa FIPS 201 del gobierno de los EEUU, así como el formato GUID de 128 bits para las credenciales PIV-I.
- Esta capacidad para usar varios tipos de tarjeta (como las de 26 bits, 37 bits o Corporate 1000)
- Memoria y respaldo RTC pila de litio CR 2032 para respaldo de RTC; las copias de seguridad de base de datos y transacciones de búfer se almacenan en memoria no volátil.
- Entradas dedicadas: Armario anti manipulación, fallo de CA, batería baja.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p>SENADO DE LA REPÚBLICA</p>	19 de 37

- El controlador deberá poder soportar hasta 256 entradas y salidas mediante módulos adicionales.
- El controlador deberá tener la posibilidad de instalación en rack o en muro.
- El controlador deberá tener la posibilidad de conectar los lectores directo mediante protocolo OSDP (al menos 8 lectores por tarjeta de comunicación) o con módulos de expansión por puerta con conexión IP
- El controlador deberá poder manejar al menos 1 bus de 8 lectoras con comunicación OSDP multi-drop.

Deberá cumplir con las siguientes normatividades:

- Access Control: UL 294, CSA C22.2 No. 205 (Canada); UL 1076, ULc 1076 (Canada)
- CE: EN 55022, EN 55024, EN 60950-1
- Safety: IEC 60950-1
- EMI: FCC Part 15 Class A, EN 55022, ICES-003(Canada), VCCI / Class A ITE (Japan), C-Tick (AS/NZS CISPR 22 - Australia/New Zealand)
- EMC: EN 55024, EN 50130-4, IEC 62599-2, EN 61000-6-1
- Encryption: FIPS 197, FIPS 201

FUENTES PARA CONTROLADOR.

El sistema de alimentación de voltaje único debe ser un cargador de batería de voltaje único y alta eficiencia, con modo de conmutación fuera de línea, diseñado como una fuente de alimentación de uso general para proporcionar alimentación ininterrumpida a cerraduras, equipos auxiliares y controladores inteligentes capaz de proveer dos salidas seleccionables entre 12 o 24 Vdc, la unidad debe contar con mecanismo de cierre con protección de tamper switch y espacio para ubicar la batería.


Las características para la fuente deben como mínimo cumplir con lo siguiente:

Entradas

- Tensión 120/230 V_{CA}, 50/60 Hz, según el modelo.
- Energía 170 W, AC máximo.
- Salidas (8 Salidas PTC)

Sistema de CC

- Tensión 12.5 / 25 V_{CC}
- Corriente 12/6 A_{CC}

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p style="text-align: center;">SENADO DE LA REPÚBLICA</p>	20 de 37

- Protección y fusibles electrónicos (15 A)
- Falla de AC.
- Salida contacto seco tipo C.
- Activación falla de alimentación de AC fusible de AC quemado.
- Baja batería.
- Salida contacto seco tipo C.
- Activación menos de 10.2 / 20.4 V_{CC}
- Carga de la batería.
- Máximo 80 Ah.
- Mínimo 2 Ah.
- Tiempo de carga de batería 80 Ah 48 horas.
- Espacio para batería en el gabinete dos baterías de 12 Ah.
- Tipo de montaje muro.
- Temperatura de operación De 0 a 50 °C (32 a 122 °F)
- Disipación del calor 66 BTU/h.
- Probado por UL294, UL603, FCC Parte 15 Subparte B.
- Probado por UL294, UL603, UL1076, FCC Parte 15, Subparte B, ULC S318, ULCS319, ULCS527 CSA C22.2#107.1, CSA 22.2 #60950 CSFM Aprobado/CE/RoHS.
- Cada fuente deberá incluir módulo de comunicación IP para monitoreo.


TARJETAS INTELIGENTES.

Se deberán suministrar tarjetas iCLASS® Seos™ de 8 K con frecuencia de funcionamiento 13.56 MHz con ISO/IEC 14443 Tipo A. Material Compuesto, 60 % PVC / 40 % PET. Formato de tarjeta con numeración única H10302.

MÓDULOS PARA CONEXIÓN LECTORAS REMOTAS CON GABINETE.

El sistema deberá incluir módulos para manejo de puertas remotas con las siguientes características:

- Puertos de lectoras por módulo uno.
- Soporte de lectoras Wiegand.
- Entradas supervisadas dos, con doble resistencia.
- Entrada de supervisión (Tamper) una.
- Salida de relevo dos, Form C contacto seco.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">21 de 37</p>

- Bus de comunicaciones RS-485 half dúplex dos cables.
- Regulaciones UL294, CE, EN50081-1, EN50130-4, EN50133, FCC Part 15 Clase A, RoHS.
- Temperatura 0 a 50 °C (32 a 122 °F)
- Humedad relativa 5 % to 95 % sin condensación.
- Capacidad del gabinete hasta dos módulos de una lectora.

LECTORAS TARJETAS INTELIGENTES.

La lectora de tarjetas inteligentes deberá poder leer los siguientes tipos de tarjetas:

- iCLASS Seos®
- iCLASS SE
- MIFARE® Classic
- MIFARE DESFire®EV1
- iCLASS® estándar
- HID Mobile Access®.

Comunicaciones con el controlador:

- OSDP V2 or Wiegand configurable.
- Certificaciones de agencias UL294/cUL (US), FCC Certification (US)
- Rango de temperatura de funcionamiento -31 a 150 °F (-35 a 65 °C)
- Rango de humedad 5 % to 95 % humedad relativa sin condensación.
- Frecuencia de transmisión 13.56 MHz.


LECTORAS DE LARGO ALCANCE.

La lectora de tarjetas inteligentes deberá poder leer los siguientes tipos de tarjetas:

- iCLASS Seos®.
- iCLASS SE.
- MIFARE® Classic.
- MIFARE DESFire®EV1.
- iCLASS® estándar.

Comunicaciones con el controlador:

- Wiegand.
- Certificaciones de agencias UL294/cUL (US), FCC Certification (US)

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">22 de 37</p>

- Rango de temperatura de funcionamiento -31 a 150 °F (-35 a 65 °C)
- Rango de humedad 5 % to 95 % humedad relativa sin condensación.
- Frecuencia de transmisión 13.56 MHz.

LECTORES BIOMÉTRICOS.

Lector biométrico con pantalla táctil color WVGA de 5 pulgadas con expansión de memoria para no menos de 50000 huellas expandible a 100000. Nivel de protección IP65. Deber ser integrable de forma nativa con la plataforma de control de acceso permitiendo el enrolamiento desde el cliente de la plataforma de control de acceso utilizando un lector tipo USB del mismo fabricante.


El equipo deberá tener las siguientes características:

- Certificaciones de agencias UL294, CE, CB, FCC. BIS.
- Rango de temperatura de funcionamiento -20 a 60 °C.
- Rango de humedad 10 % to 80 % humedad relativa sin condensación.
- Lector de tarjeta sin contacto en opción iClasss®.
- Modos de comunicación con controlador OSDP y Wiegand.
- Alimentación *Power Over Ethernet* (POE)
- Sistema operativo Linux.
- Procesador ARM® Cortex™-A9 core 1GHz.

ESTACIÓN CLIENTE DE ENROLAMIENTO Y CARNETIZACIÓN.

Cada estación cliente deberá contar con los siguientes elementos:

- Un Computador de marcas comerciales como DELL, HP o Lenovo con las características de ESTACIÓN DE TRABAJO descritas en el presente documento.
- Monitor LCD de 22 pulgadas resolución FHD 1920x1080 con entradas HDMI, VGA y BNC.
- Escáner de enrolamiento biométrico con sensor óptico (23 x 23 mm, 500 dpi, 256 niveles de gris) con puerto USB del mismo fabricante de las lectoras biométricas. Incluye licencias y software necesario.
- Escáner de documentos USB, permita capturar información de pasaportes y documentos de identidad, deberá ser compatible de forma nativa con el software de control de accesos. 600 DPI o superior. Incluir licencia para OCR.
- Almohadilla para firma electrónica con conexión USB. Área para firma 121 mm x 25 mm. Deberá ser compatible de forma nativa con el software de control de accesos
- Cámara web USB para toma de fotografías. Resolución 720 x 480 a 30 fps, 1/3 pulgadas CCD Sensor: Lente fijo 6 mm f/1.8 montaje CS.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">23 de 37</p>

- Impresora de tarjetas. Resolución 300 dpi, 16.7 millones de colores. Capacidad 100 tarjetas en la tolva de entrada y salida. Conexión USB y Ethernet. Temperatura de operación 18 °C – 27 °C. Deberá incluir 26 cartuchos de repuesto color YMCKO con resina y 31 cartuchos de limpieza.

SISTEMA DE GESTIÓN DE VIDEO

GENERALIDADES

El software de Sistema de Administración de Video (VMS) se utilizará para visualizar video en vivo y grabado desde dispositivos IP conectados a redes de área local o amplia. El software VMS deberá estar basado en una arquitectura cliente/servidor que pueda configurarse como un sistema VMS independiente con el software cliente que se ejecute en el hardware de servidor y/o el cliente que se ejecute en cualquier estación de trabajo TCP/IP conectada a la red. Varias estaciones de trabajo cliente deben poder visualizar video en vivo o grabado desde un servidor o varios servidores de manera simultánea. Varios servidores también deben poder proporcionar video en vivo o grabado a una o más estaciones de trabajo.

El Senado de la República ya cuenta con Cámaras de Video IP de diferentes marcas las cuales se deben utilizar, el cálculo de video se realizará para 290 cámaras todas configuradas a mínimo 4 megaPixel, mínimo 15 cuadros por segundo, grabación continua por 8 horas y restante por detección de movimiento con actividad de la escena alta, para 180 días mínimo por cámaras en formato H265, se deben entregar los cálculos de video de almacenamiento y tasa de transferencia efectiva (throughput) correctos y calculados correctamente.

El Senado de la Republica actualmente cuenta con equipos NAS por 600 TB los cuales deben ser usados en el sistema ofertado para almacenar video y suministrar el almacenamiento restante, este deberá usarse como extensor de disco de los NVR ofertados realizando la respectiva configuración de Red.

El sistema deberá contar con un sistema de respaldo y contingencia failover de tal forma que si alguno de los NVR llegara a fallar entre un grabador de respaldo a soporta la grabación.


ADMINISTRADOR DE VIDEO.

El VMS no deberá aplicar cargos por la cantidad de clientes concurrentes ni cobrará por adición de clientes futuros.

EL VMS deberá permitir actualización de los clientes totalmente gratis de forma vitalicia.

EL VMS deberá permitir la actualización mínima del software server y demás software asociados mínimo por los siguientes 5 años sin cobros adicionales.

El VMS deberá ser compatible con formato H265 y H265+

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	24 de 37

El sistema VMS deberá utilizar: servidores desarrollados por fabricantes, estaciones de trabajo de PC comerciales listos para usar, servidores, dispositivos de red y equipos de almacenamiento.

La grabación de todo el video que se transmite al VMS será continua, ininterrumpida y sin supervisión.

El sistema VMS deberá tener la capacidad de grabación de video por detección de movimiento de la cámara, de manera que dicho video se graba cuando el software de administración de video detecta movimiento dentro de un área de interés de la visión de la cámara. El video anterior a la detección de movimiento se debe almacenar también mediante el uso de la función pre-grabado.

El sistema VMS administrará el video para el cual fue configurado a monitorear. La pérdida de señal de video se debe configurar para anunciar en el cliente VMS mediante una indicación visual en pantalla que alerta a los operadores acerca de la pérdida de video.

EL software VMS software deberá tener una arquitectura abierta compatible con cámaras IP y codificadores de varios fabricantes donde se hubiera desarrollado un driver de compatibilidad con la cámara a integrar además de la compatibilidad ONVIF, brindando así la compatibilidad en video, entradas y salidas, audio etc. de cada cámara integrada, desde funciones básicas de bajo costo hasta funciones de mega píxeles de alta resolución.

El software cliente VMS debe poder visualizar video y audio en vivo, video y audio grabado y permita configurar todo el sistema desde una única aplicación.

El VMS debe continuar grabando video y audio en todo momento durante la administración y configuración de cualquier función.

El VMS deberá monitorear la salud total del sistema suministrado como estado de discos duros, fuentes de alimentación de los NVR's, cámaras conectadas o desconectadas e informar en un reporte sencillo y liviano.


El VMS deberá tener la capacidad de informar al operador de forma sencilla y gráfica cuando se genere una actualización del parte de fábrica y alguno de los NVR's esté desactualizado.

El VMS deberá gestionar la actualización centralizada de los NVR's

El software cliente VMS debe tener la misma funcionalidad cuando se encuentra conectado de forma remota como cuando se ejecuta de manera local en la misma computadora como el software de servidor.

El software cliente VMS añadirá y eliminará funciones basado en permisos del usuario y la funcionalidad que disponga de licencia

El software cliente VMS debe funcionar en todos los siguientes sistemas operativos:

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p style="text-align: center;">SENADO DE LA REPÚBLICA</p>	25 de 37

- Microsoft Windows 2012/2012 R2 /2016.
- Microsoft Windows 7 Pro.
- Microsoft Windows 8.1.
- Microsoft Windows 10.
- Linux Ubuntu 16.04/ 18.04.
- Apple Mac OS 10.7 a 10.13.

El software VMS debe permitir al usuario tener cualquier combinación de aplicaciones cliente VMS que se ejecuten en cualquiera de los sistemas operativos compatibles y conectarse a cualquiera de los servidores VMS que se ejecute en cualquiera de los sistemas operativos compatibles. Por ejemplo, un cliente VMS que se ejecuta en Microsoft Windows 10 debe poder conectarse de forma simultánea a tres (3) servidores VMS diferentes que se ejecutan en diferentes sistemas operativos, como Windows Server, Windows 10 o Linux.

La interfaz web cliente debe funcionar sin la necesidad de la instalación de software alguno mediante los siguientes exploradores:

- Internet Explorer 6 y versiones posteriores.
- Firefox 2 y versiones posteriores.
- Opera 9 y versiones posteriores.
- Safari y versiones posteriores.
- Chrome.

El software de servidor VMS debe grabar y obtener datos de video, audio y alarmas y los enviará a los clientes VMS si así se lo solicita.


El software VMS debe proporcionar sin cargo alguno una aplicación móvil diseñada expresamente capaz de visualizar de forma simultánea transmisiones de video en vivo y reproducir una transmisión de video grabada. La aplicación se debe proporcionar para los sistemas iOS y Android (incluido Kindle Fire)

El servidor VMS no debe decodificar video para los fines de detección de movimiento.

El servidor VMS no debe decodificar video con el fin de volver a empaquetarlo para la transmisión a los clientes.

El software de servidor VMS debe funcionar en cualquiera de los siguientes sistemas operativos:

- Microsoft Windows Server 2008R2/2012/2012 R2 /2016
- Microsoft Windows 7 Pro
- Microsoft Windows 8.1

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	26 de 37

- Microsoft Windows 10
- Linux Ubuntu 14.04 / 16.04/ 18.04

El VMS debe otorgar la licencia para todas las cámaras en el sistema. La licencia se debe basar en la dirección MAC de una única tarjeta de red presente en el sistema. El VMS solo debe requerir que la tarjeta de red se encuentre habilitada y no requiere que realmente se envíen datos a través de ella.

El VMS no debe requerir que se contacte al fabricante cuando falla una cámara.

El software de servidor VMS se debe ejecutar como un servicio. VMS no debe requerir que se ejecute una aplicación para funcionar.

El VMS debe permitir el uso de mapas. Los usuarios debe poder acceder a los mapas con los niveles de permisos apropiados y mostrar las fuentes de video y sus estados.

El VMS deberá permitir colocar disparadores, visualizados y accionados desde un mapa.


El software VMS debe permitir el uso de la integración de una línea de comando. La línea de comando permitir la llamada del video apropiado cuando se lo solicite mediante el uso de la función de línea de comando.

El software VMS debe admitir el uso de una lente panorámica en una cámara análoga o IP. El cliente VMS debe corregir la distorsión de la imagen tanto en el video en vivo como en el video grabado.

En el modo en vivo, el usuario debe poder ver video en vivo, audio en vivo e información sobre alarmas.

El VMS deberá organizar el panel de vista de video de cámara en los siguientes patrones:

- Presentación de 1 cámara (pantalla completa)
- Presentación de 4 cámaras (2x2)
- Presentación de 8 cámaras (3 vistas grandes y 4 vistas pequeñas)
- Presentación de 10 cámaras (2 vistas grandes y 8 vistas pequeñas)
- Presentación de 13 cámaras (1 vistas grande y 12 vistas pequeñas)
- Presentación de 16 cámaras (4x4)
- Presentación de 8 cámaras (1 vista muy grande y 7 vistas pequeñas)
- Presentación de 9 cámaras (3x3)
- Presentación de pantalla ancha de 6 cámaras (2x3)
- Presentación de pantalla ancha de 12 cámaras (4x3)
- Presentación de pantalla ancha de 20 cámaras (5x4)

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	27 de 37

- Presentación de pantalla ancha de 30 cámaras (6x5)
- Presentación de pantalla ancha de 48 cámaras (8x6)

El VMS debe brindar una opción para visualizar paneles de pantallas de video anchas de 16:9.

El VMS debe permitir la personalización de la interfaz de usuario para que se visualicen los disparadores de software. Esto debe permitir a los usuarios activar eventos mediante la pulsación de un botón, lo que podría disparar la grabación, los valores preestablecidos de giro, inclinación y zoom (PTZ, Pan-TiltZoom), los disparadores de salida, o el correo electrónico.

El VMS debe permitir al usuario elegir su propio ícono y seleccionar los disparadores de software para presentar en el cliente. VMS también debe mostrar el estado de cualquier disparador suave activado conectado a los servidores VMS.

El software VMS debe permitir el control de las cámaras PTZ a los usuarios autorizados y ser utilizado para maniobrar una cámara PTZ. Cuando se lo utiliza en una cámara que no es PTZ, le permitir girar, inclinar y hacer zoom de forma digital en cualquier video ya sea en modo en vivo o modo grabado.


El VMS debe permitir los siguientes métodos para controlar una cámara PTZ para que se encuentre disponible:

- Ventanas de control de gráficos PTZ.
- Íconos activos de control PTZ de superposición de gráficos.
- Control de teclado (flechas arriba, abajo, izquierda, derecha; página arriba, página abajo para zoom)
- Valores preestablecidos de PTZ.
- PTZ digital.
- Joystick USB para controlar cámaras PTZ.
- Control PTZ proporcional al hacer clic con el mouse en el centro y moverlo.

El software VMS debe permitir la función matriz virtual al designar una celda para hacerlo. Esta celda de video debe mostrar el video de forma automática cuando se le dispere.

El software VMS debe tener una función para visualizar grupos lógicos de cámaras. Esto debe permitir la visualización eficiente de cámaras en un orden lógico.

El software VMS debe tener una función para organizar sus cámaras en vistas preestablecidas. Las vistas son disposiciones de los paneles de video configurados previamente que puedan ser seleccionados fácilmente más adelante. Una vista deberá guardar la ubicación de las vistas de las transmisiones de video, las transmisiones de audio,

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	28 de 37

los datos del punto de venta, los mapas y de eventos. Se debe poder acceder a estas vistas en los modos de video en vivo y grabado.

El software VMS debe poder desplazarse automáticamente por dos o más vistas guardadas para crear un tour de video. VMS debe permitir la configuración del tiempo de espera y las diferentes vistas que utilizará.

El software cliente VMS se utilizará para buscar y reproducir video, audio y eventos grabados desde servidores VMS.

El software VMS debe tener la capacidad de buscar y reproducir video desde varias cámaras de forma simultánea. Todo el video grabado se debe reproducir y mostrar en una presentación sincronizada de varias cámaras.

El software permitir la búsqueda en el video grabado basado en la hora, fecha, fuente de video, región de imagen y que los resultados se muestren tanto como una línea de tiempo en la que se puede hacer clic y como una serie de imágenes en miniatura. A su vez el sistema debe permitir la búsqueda y reproducción de audio en sincronización con el video.

El software VMS debe permitir buscar en un área específica de video grabado y solo mostrar los cuadros en los que el movimiento ocurrió en esa área.

El software VMS debe tener la capacidad de exportar video, mapas, datos del punto de venta y archivos de audio.


El software VMS debe brindar la opción de exportar el archivo en los siguientes formatos:

- Exe independiente (*.exe) – incluye un reproductor ejecutable con los datos de video y audio.
- Archivo AVI (*.avi) – un formato de contenedor multimedia.
- Archivo PS (*.ps) – un formato para la multiplexación de audio y video.
- Archivo QuickTime (*.mov) – nativo para computadoras Macintosh.

El reproductor VMS independiente debe empaquetar todo el video exportado en un ejecutable único. El reproductor VMS independiente debe poder autenticar que el video no fue adulterado.

El software cliente VMS debe poder conectarse a varios sistemas de forma simultánea. Cada sistema podría tener permisos individuales, por lo que se limitan las capacidades de configuración o visualización del cliente para ese sistema, pero no afecta las capacidades con respecto a otros sistemas.

El sistema VMS debe poder mostrar información del sistema sobre los usuarios que han iniciado sesión en el sistema, número de información de versión del archivo plug-in y estado

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p>SENADO DE LA REPÚBLICA</p>	29 de 37

y un registro del sistema que contiene un historial detallado del proceso que ocurre en el sistema.

El sistema VMS debe tener la capacidad de grabar un registro de auditoría del momento en que los usuarios inician sesión que muestra los cambios que realizaron, los videos que visualizaron y los archivos que exportaron.

El sistema VMS debe permitir realizar la configuración de los dispositivos de video en el cliente, y enviarla a los dispositivos. La configuración en sí se debe almacenar tanto en la cámara como en el VMS.

El VMS permitir el monitoreo de las entradas tanto en los dispositivos de red como en el hardware provisto por fabricantes. El VMS también debe permitir el disparo de salidas en los dispositivos de red y en el hardware provisto por fabricantes.

El VMS debe permitir la configuración de las unidades que se deben utilizar para la grabación de video. Dichas unidades pueden ser unidades locales, unidades de almacenamiento con conexión directa.

VMS debe permitir la configuración de reglas para la grabación de video. Estas reglas le deben permitir establecer una cantidad máxima de días o una cantidad mínima de días por transmisión de video.

El VMS no debe requerir una base de datos para la grabación de video.

El VMS debe tener la capacidad para recibir datos ASCII a través del puerto COM en el servidor, o a través de la red.


El VMS debe tener la capacidad para realizar la búsqueda de palabras clave en los datos ASCII y luego utilizarlos para ejecutar varios eventos como valores preestablecidos de PTZ, grabación de video, grabación de audio y el envío de notificaciones por correo electrónico.

El software VMS debe poder enviar un correo electrónico definido previamente basado en un disparador de eventos. El software VMS también debe admitir conexiones SSL y TLS para las transmisiones de correo electrónico.

El software VMS debe tener una función para exportar un segmento de video desde cámaras específicas o entradas de audio a un CD o DVD en función de la activación un disparador de entrada u otro evento.

El software VMS se utilizará para conectar diferentes tipos de eventos, como disparadores de entrada, a una acción deseada como la grabación de video o el disparo de una alarma. El software VMS reconocerá los siguientes tipos de eventos:

- Movimiento de video
- Pérdida de video

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	30 de 37

- Disparador de entrada
- Conexión de Cámara IP
- Disparador de software
- Análisis

El software VMS debe poder ejecutar los siguientes tipos de acciones:

- Grabación de video
- Disparador de salida
- Video de salida
- Envío de un correo electrónico
- Grabación de CD/DVD
- Invocar un valor preestablecido de PTZ

El software VMS debe tener la capacidad para configurar el tiempo de grabación de cada entrada de video por hora. Esto debe permitir al usuario programar el momento en el que se grabará por movimiento, por evento o cuando no realiza una grabación.

El VMS utilizará una combinación de nombre de usuario y contraseña para autenticar el nivel de permiso del usuario.

El VMS debe permitir la granularidad de permisos al crear grupos de usuarios personalizados. Los miembros de estos grupos de usuarios personalizados debe tener todos los mismos permisos.

El VMS debe permitir al usuario realizar una búsqueda visual por miniaturas. El usuario debe poder seleccionar una cámara para ver una imagen por un período de tiempo establecido. El usuario debe poder reproducir video desde esa imagen o/y acercar durante un periodo de tiempo.

El cliente VMS debe poder configurarse para cambiar vistas automáticamente en base a cualquier disparador dentro de la función de monitoreo de eventos.

El VMS deberá poder generar marcadores en el video para identificación de eventos relevantes y manejo de casos para investigaciones. Se deberá poder exportar el video de múltiples cámaras a la vez.

El entorno grafico del VMS deberá poder manejar mapas anidados para rápida navegación de acuerdo a la ubicación física de la cámaras.

Se deberá poder monitorear el estado de todos los NVR y cámaras mediante un tablero grafico de alarmas y eventos.

El VMS deberá poder manejar redundancia de los NVR de uno a varios.


 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	<p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p> <p>SENADO DE LA REPÚBLICA</p>	31 de 37

El Senado cuenta actualmente con sistema de almacenamiento masivo tipo NAS operativos los cuales deberán ser integrados al VMS para ampliar la capacidad de grabación y archivo extendido de video.

Se deben integrar las cámaras existentes y que serán instaladas en el Senado. El suministro de cámaras no es parte del alcance de este proceso.

EQUIPO GRABADOR PRINCIPAL ESPECIFICACIONES TÉCNICAS

- El NVR deberá soportar video simultáneo para clientes locales con 700 fps de video.
- El NVR debe poder conectar mínimo 500 clientes remotos.
- Deberá tener interfaces de red de 10 Gbps duales para rápido almacenamiento o mejorar el rendimiento de los clientes conectados.
- El NVR deberá tener fuente redundante para grabación continua en caso de una falla en la fuente de alimentación.
- El NVR debe utilizar discos duros de clase empresarial y deberá soportar cambios en caliente.
- El NVR deberá contar con operación ininterrumpida y preservación del video en uno o más discos duros en caso de que alguno falle.
- El NVR deberá tener opción de conmutación de discos duros en caso de que alguno falle.
- Debe soportar discos duros de estado sólido que operen en sistemas operativos
- El NVR deberá soportar mínimo 128 cámaras IP.
- El NVR deberá ser compatible con diferentes modelos y marcas de cámaras IP del mercado.
- El NVR deberá tener capacidad de grabación de 240 TB raid 6.
- El NVR deberá contar con un mínimo de 800 Mbps de rata de almacenamiento de video
- El NVR deberá tener como mínimo salidas de video DVI-I, HDMI, VGA.
- El NVR deberá soportar como mínimo 2 monitores simultáneamente
- El NVR deberá trabajar sobre Windows 10, 64 bit.
- El NVR deberá tener puerto serial RS485/RS232
- El NVR deberá tener mouse y teclado incluido
- El NVR deberá tener como mínimo 8 puertos USB
- El NVR deberá cumplir con las siguientes certificaciones: CE, FCC, ULus, UL Listed
- El NVR deberá tener fuente redundante
- Procesador y Memoria RAM: E3-1275 Xeon CPU y 16 GB ECC.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">32 de 37</p>

- El oferente deberá garantizar la actualización de versiones que se requieran para su funcionamiento sin costo alguno para la entidad en el periodo de garantía.
- El NVR deberá incluir la totalidad de las licencias necesarias para la puesta en funcionamiento del sistema sin costo alguno para la entidad
- El NVR deberá ser de tipo montaje en rack
- El NVR deberá incluir derecho a actualizaciones mínimo por 5 años sin costos adicionales

EQUIPO GRABADOR RESPALDO ESPECIFICACIONES TÉCNICAS

- El NVR deberá soportar video simultáneo para clientes locales con 700 fps de video.
- El NVR debe poder conectar mínimo 500 clientes remotos.
- El NVR deberá tener la opción de fuente redundante para grabación continua en caso de una falla en la fuente de alimentación.
- El NVR debe utilizar discos duros de clase empresarial y deberá soportar cambios en caliente.
- El NVR deberá contar con operación ininterrumpida y preservación del video en uno o más discos duros en caso de que alguno falle.
- El NVR deberá tener opción de conmutación de discos duros en caso de que alguno falle.
- Debe soportar discos duros de estado sólido que operen en sistemas operativos
- El NVR deberá soportar mínimo 128 cámaras IP.
- El NVR deberá ser compatible con diferentes modelos y marcas de cámaras IP del mercado.
- El NVR deberá tener capacidad de grabación de 48 TB raid 5.
- El NVR deberá contar con un mínimo de 800 Mbps de rata de almacenamiento de video
- El NVR deberá tener como mínimo las siguientes salidas de video, 1 DVI-I, 1 HDMI, 1 VGA
- El NVR deberá soportar como mínimo 2 monitores simultáneamente
- El NVR deberá trabajar sobre Windows 10 64 bit,
- El NVR deberá tener puerto serial RS485/RS232
- El NVR deberá tener mouse y teclado incluido
- El NVR deberá tener como mínimo 8 puertos USB
- El NVR deberá cumplir con las siguientes certificaciones: CE, FCC, ULus, UL Listed
- El NVR deberá tener fuente redundante

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	ANEXO TÉCNICO	Página
	SENADO DE LA REPÚBLICA	33 de 37

- El oferente deberá garantizar la actualización de versiones que se requieran para su funcionamiento sin costo alguno para la entidad en el periodo de garantía.
- El NVR deberá incluir la totalidad de las licencias necesarias para la puesta en funcionamiento del sistema sin costo alguno para la entidad
- El NVR deberá ser de tipo montaje en rack
- El NVR deberá incluir derecho a actualizaciones mínimo por 5 años sin costos adicionales

TECLADO CONTROLADOR PARA MANEJO DEL VMS Y CONTROL CÁMARAS PTZ.

El teclado de control de cámaras deberá tener conexión USB con la estación de trabajo. Compatible con sistemas operativo Windows, Linux y Mac. El equipo deberá ser del mismo fabricante del VMS garantizando máxima compatibilidad. El teclado deberá contar con palanca de mando de tres ejes de efecto Hall X / Y / Z para control de posicionamiento. Recorrido de la palanca de mando: eje X / Y +/- 18°, eje Z +/- 40°. Eje de la palanca de mando: acero inoxidable. 27 botones de operación 11 con funciones fijas y 16 configuradas por el usuario.


Certificaciones de agencias CE, FCC, RoHS

Rango de temperatura de funcionamiento 25 °C a 85 °C

SISTEMAS DE ANALÍTICA DE VIDEO.

Se deben incorporar equipos de cómputo dedicados para analítica de video que sean completamente compatibles con la solución de VMS. Deben tener las siguientes características mínimo para 32 cámaras:

- 4 canales para el reconocimiento de placas de vehículos o hasta 16 canales para video inteligencia según la resolución del flujo de video.
- Un puerto LAN 10/100/GE full dúplex.
- Intel Core i5 vPro.
- Disco duro SSD de 500 GB.
- Disco duro SATA II de 1 TB, 63.5 mm (2.5 pulgadas), 5400 rpm.
- Cumplimiento regulatorio: EN 60950, IEC 60950 FCC Parte 15, Clase A; EN 55022; EN 55024; EN 50130-4; AS/NZS CISPR 22; ICES-003 Clase A, RoHS/WEEE.
- Reglas de video inteligencia:
 - Filtrado por color
 - Formación de aglomeraciones
 - Dirección
 - Permanencia

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">34 de 37</p>

- Ingreso/egreso
- Abandono de objetos
- Remoción de objeto
- Merodeo

REQUERIMIENTOS MÍNIMOS DE LICENCIAMIENTO Y GARANTÍA.

Para todos los componentes de la solución: Garantía de soporte y repuestos a cinco (5) años en modalidad 7x24.

Para todos los componentes de la solución: Soporte telefónico de fabricante y en sitio de parte del oferente cuando se requiera durante cinco (5) años.

El oferente deberá anexar certificación del fabricante donde evidencie que es distribuidor autorizado y enumerando la plataforma ofertada para el presente proyecto.

El proveedor deberá indicar claramente el tipo de licenciamiento necesario para poder crecer en cada uno de los dispositivos ofertados. Las licencias entregadas para tal fin deben ser a perpetuidad

CONDICIONES DE PRESTACIÓN DE SERVICIO DE SOPORTE, MANTENIMIENTO CORRECTIVO Y REEMPLAZO DE PARTES EN SITIO.

Las condiciones de prestación de servicio son las siguientes:

- Mantenimiento correctivo y reemplazo de partes en sitio.
- Un mantenimiento preventivo al año.
- Duración de la garantía 5 años.

Prestar el servicio de atención telefónico y en sitio, en modalidad 7x24 (7 días a la semana, 24 horas al día, 365 días al año), para la recepción de solicitudes de servicio generadas por el personal de TI que el Senado designe.

La atención y solución de los casos deberá ajustarse a las prioridades y tiempos de respuesta definidos por el Senado en la siguiente tabla:

Prioridad	Tiempo de atención telefónica	Tiempo de respuesta remota	Tiempo de Atención en sitio
Prioridad Alta	1/2 hora	1 hora	4 horas
Prioridad Media	1 hora	2 horas	8 horas
Prioridad Baja	2 horas	8 horas	Programado

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">35 de 37</p>

Las prioridades de los casos de atención se clasificarán a criterio del personal de TI que el Senado designe, según la severidad del incidente de acuerdo con la siguiente tabla:

Prioridad Alta	Prioridad Media	Prioridad Baja
<p>El equipo se encuentra fuera de servicio, El equipo no puede ser utilizado debido a fallas en su funcionalidad o a pérdidas de datos, El equipo es ineficiente o muy lento en su operación, Detección de vulnerabilidades que ponen en riesgo la seguridad del sistema</p>	<p>El equipo presenta fallas serias del sistema operativo, pero son predecibles y manejables por parte del administrador.</p> <p>Degradación del rendimiento del sistema que no compromete el desempeño global del clúster, El equipo presenta defectos o errores que causan un impacto limitado o nulo sobre el desempeño y funcionalidad de los sistemas de información,</p>	<p>Preguntas, configuraciones y/o actualizaciones que requieren de soporte técnico,</p> <p>Cambios en las configuraciones de hardware y/o software que se requieran para asegurar la prestación del servicio,</p>


Se deberá incluir el soporte con la fábrica para abrir casos, instalación de parches y/o actualizaciones que libere el fabricante durante la vigencia del contrato, las cuales deberán ser implementadas por el contratista.

En caso de fallas de hardware, el contratista enviará una parte de reemplazo que supla funcionalmente las características del equipo en daño en un tiempo no mayor a 24 horas de realizada la solicitud del repuesto.

MANTENIMIENTO PREVENTIVO.

Se deberá ejecutar un programa de mantenimiento preventivo anual para todos los equipos incluidos en el contrato. Se deberá entregar a la entidad un cronograma con las fechas estimadas para la ejecución del mantenimiento preventivo de los equipos, el cual será acordado con el Senado una vez asignado el contrato.

Al finalizar cada mantenimiento preventivo se deberá entregar a la entidad un reporte detallado de los equipos atendidos, en el cual se incluyan las características técnicas básicas: modelo, versiones de software, numero de inventario interno del Senado, numero serial, espacio, edificio, e identificación del stack.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">36 de 37</p>

El contrato deberá incluir el derecho para la entidad a utilizar todas las actualizaciones de software y firmware que se liberen durante su vigencia. El contratista deberá instalar estas actualizaciones durante los mantenimientos preventivos o cuando la entidad lo requiera según la necesidad de la solución.

CONDICIONES DE ATENCIÓN.

El proponente deberá contar con una línea telefónica local en la ciudad de Bogotá, o una línea gratuita nacional 01-8000 para el registro y atención de las solicitudes de servicio de los equipos amparados, en modalidad 7x24x365.

El proponente deberá estar acreditado como canal autorizado en Colombia de los equipos de red y contar con personal certificado del fabricante.

Tener a disposición del Senado, personal técnico requerido para la apropiada ejecución de los servicios. En caso de requerirse personal adicional para ejecución de los requerimientos, el contratista deberá contar con los mecanismos necesarios para que presten el servicio de forma coordinada.

Se deberá coordinar con el personal de TI que la entidad designe, la atención de las solicitudes de soporte y la programación de los mantenimientos preventivo y/o correctivo, los cuales deben ser atendidos de acuerdo al grado de prioridad señalado al momento de registrar el caso.

DOCUMENTOS Y CERTIFICACIONES REQUERIDOS.

Anexar carta de certificación del fabricante de la solución ofertada donde se acredite al proponente como canal autorizado en Colombia para la venta de los productos ofertados, y certificación al mayorista como distribuidor directo autorizado en Colombia, dichas certificaciones que deben ser expedidas por el fabricante. No se aceptan certificaciones a través de mayoristas. En caso de participar mediante consorcios o uniones temporales, esta certificación solo se le exigirá a uno de los miembros de dicha unión.

Anexar original o copia del Certificado de Cámara de Comercio donde conste que el fabricante de la solución de está constituido como firma en Colombia por mínimo cinco (5) años anteriores a la presentación de la oferta.

El proponente deberá anexar certificación ISO 9000 del fabricante de la solución.

Presentar documento donde se especifique las condiciones de garantía, soporte y mantenimiento durante los cinco (5) años posteriores al recibo de la solución.

Presentar cronograma detallado del proyecto indicando recursos y personal asignado en cada etapa.

SERVICIOS DE CAPACITACIÓN.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA</p>	<p align="center">ANEXO TÉCNICO</p> <p>ESPECIFICACIONES TÉCNICAS PARA CONTRATAR LA RENOVACIÓN DEL SISTEMA DE CONTROL DE ACCESO, MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA OPERACIÓN DEL INGRESO DE FUNCIONARIOS Y VISITANTES DEL SENADO DE LA REPÚBLICA.</p>	<p align="center">Página</p>
	<p align="center">SENADO DE LA REPÚBLICA</p>	<p align="center">37 de 37</p>

El Senado requiere de capacitación conducente a certificación para la administración de Sistemas Operativos BSD o Linux. (Incluyendo desplazamiento y viáticos). Esta capacitación no generará costos adicionales para la entidad y no deberá adicionarse o separarse como ítem discriminado a la tabla de costos de la oferta. La capacitación deberá incluir la certificación.