# GENERAL

## DESCRIPCIÓN DEL SISTEMA

### Requisitos generales

#### La unidad especificados deberán formar parte de la línea oficial de productos del fabricante, diseñada para uso comercial y/o industrial 24/7/365.

#### La unidad especificada deberá basarse en componentes estándares y tecnología comprobada usando protocolos abiertos y publicados.

### Sostenibilidad

#### La unidad especificada deberá fabricarse de conformidad con la norma ISO 14001.

#### La unidad especificada deberá cumplir con las directivas de la UE 2011/65/EU (RoHS) y 2012/19/EU (WEEE).

#### La unidad especificada deberá cumplir con la regulación de la UE 1907/2006 (REACH).

## CERTIFICACIONES Y ESTÁNDARES

### Abreviaciones generales y acrónimos

#### AES: *Advanced Encryption Standard*, Estándar Avanzado de Encriptación

#### API: *Application Programming Interface*, Interfaz de Programación de Aplicaciones

#### Tasa de bits: La cantidad de bits por unidad de tiempo enviados en una red.

#### DHCP: *Dynamic Host Configuration Protocol*, Protocolo de Configuración Dinámica del Host.

#### DNS: *Domain Name System*, Sistema de Nombres de Dominio.

#### FPS: *Frames per Second*, Cuadros por Segundo.

#### FTP: File Transfer Protocol, Protocolo de Transferencia de Archivos

#### H.264 (Formato de compresión de videos)

#### IEEE 802.1x: Marco de autenticación para dispositivos en la red.

#### IP: *Internet Protocol*, Protocolo de Internet.

#### Luz IR: luz infrarroja.

#### ISO: *International Standards Organization*, Organización Internacional de Normalización.

#### JPEG: Joint Photographic Experts Group (formato de imágenes)

#### LAN: *Local Area Network*, Red de Área Local.

#### LED: *Light Emitting Diode*, Diodo Emisor de Luz.

#### MPEG: Moving Picture Experts Group (formato de video).

#### Multicast: comunicación entre un único emisor y múltiples receptores en una red.

#### NTP: *Network Time Protocol*, Protocolo de Tiempo de Red.

#### ONVIF: Estándar global para la interfaz de productos de seguridad físicos basados en la tecnología IP.

#### PACS: *Physical Access Control System*, Sistema de Control de Acceso Físico.

#### PoE: *Power over Ethernet* (IEEE 802.3af/at), estándar para el suministro energía por el cable de red.

#### Escaneo Progresivo: Una tecnología de escaneo de imágenes que escanea todo el cuadro.

#### QoS: *Quality of Service*, Calidad del Servicio.

#### RPC: *Remote Procedure Call*, Llamada a Procedimiento Remoto

#### SIP: *Session Initiation Protocol*, Protocolo de Inicio de Sesión

#### SMTP: *Simple Mail Transfer Protocol*, Protocolo para la Transferencia Simple de Correo

#### SNMP: *Simple Network Management Protocol*, Protocolo Simple de Administración de Red

#### SSL: Secure Sockets Layer, Capa de Sockets Seguros

#### TCP: Transmission Control Protocol, Protocolo de Control de la Transmisión

#### TLS: Transport Layer Security, Seguridad de la Capa de Transporte

#### Unicast: Comunicación entre un único emisor y un único receptor en una red.

#### UPS: *Uninterruptible Power Supply*, Fuente de Alimentación Ininterrumpible

#### VBR: Variable Bit Rate, Tasa de Bits Variable

#### VMS: Video Management System, Sistema de Gestión de Video

#### WDR: Wide dynamic range, Rango dinámico amplio

### La unidad especificados deberán tener las siguientes aprobaciones de EMC:

#### EN55032: 2012

#### EN55024: 2010

#### 2014/35/EU

#### 2014/30/EU

#### 2012/19/EU

#### 2011/65/EU

#### EN 55032 Clase A

#### EN 55032 Clase B

#### EN 55024

#### FCC Parte 15 - Subparte B Clase A

#### FCC Parte 15 - Subparte B Clase B

#### FCC Parte 15 - Subparte B Clase A + B

#### ICES-003 Clase A

#### ICES-003 Clase B

### La unidad especificados deberán cumplir con los siguientes estándares de seguridad del producto:

#### IEC/EN/UL 60950-1

### La unidad especificados deberán cumplir con los siguientes estándares:

#### Audio:

##### G.711

##### G.729

##### G.722 (banda ancha)

##### L16 / 16kHz (banda ancha)

#### Video:

##### H.263+

##### H.263

##### H.264 (MPEG-4 AVC)

##### MPEG-4 Parte 2

##### MJPEG

#### Interconexión:

##### IEEE 802.3af/802.3at (Power over Ethernet)

##### IEEE 802.1X (Autenticación)

##### IPv4 (RFC 791)

##### QoS

#### Entorno mecánico:

##### IEC/EN 60529 IP65

##### IEC/EN 62262 IK07

## ASEGURAMIENTO DE CALIDAD

### El Contratista o los sub-contratistas de seguridad deberán ser Contratistas de seguridad con licencia, con un mínimo de cinco (5) años de experiencia instalando y haciendo servicio a sistemas con alcance y complejidad similares, y debe presentar evidencia de que ha completado al menos tres (3) proyectos con un diseño similar y que actualmente está involucrado en la instalación y el mantenimiento de los sistemas aquí descritos.

### Todo trabajo relacionado con la instalación, configuración, ajustes, programación y afines deberá ser realizado por técnicos electrónicos debidamente entrenados por el fabricante para la instalación y el servicio del equipo suministrado.

### El contratista o sub-contratista designado deberá suministrar credenciales que demuestren haber completado la certificación del fabricante, verificadas por una organización de terceros, como prueba de su conocimiento.

### El Contratista deberá suministrar cuatro (4) referencias actuales de clientes con sistemas de alcance y complejidad similares que se hayan puesto en marcha en los últimos tres (3) años. Al menos tres (3) de estas referencias deberán ser usando los mismos componentes del sistema, en una configuración similar a la del sistema propuesto.

### La unidad especificados deberán ser fabricados de conformidad con la norma ISO9001.

## GARANTÍA

### Todos los componentes del sistema de seguridad y la mano de obra realizada por el contratista, incluyendo el cableado, software, hardware y partes personalizadas, deberán tener una garantía total que incluya partes, materiales, mano de obra y gastos de viaje por un mínimo de tres (3) años.

### El fabricante deberá suministrar una garantía y una garantía extendida opcional para la unidad por un período total máximo de cinco años. Si se dicta como parte del contrato, el contratista reparará o sustituirá partes y/o mano de obra de conformidad con la garantía por el plazo de la misma sin incurrir en costos adicionales para el cliente.

# PRODUCTOS

## General

### Los intercomunicadores deben ser basados en tecnología IP y cumplir con los estándares de red y video establecidos.

### Los intercomunicadores deben recibir la alimentación del switch usando el cable de red.

### Los intercomunicadores deben ser completamente soportados por una API (Interfaz de Programación de Aplicaciones) abierta y publicada, la cual deberá suministrar la información necesaria para la integración de la funcionabilidad con aplicaciones de terceros.

## PROGRAMA DEL INTERCOMUNICADOR

### Los tipos de intercomunicadores listados a continuación que describen varias resoluciones, factores de formas y características deberán ser suministrados por un único fabricante de intercomunicadores.

### La fabricación de los intercomunicadores y los números de modelos serán los siguientes:

#### El intercomunicador IP modular deberá ser el 2N IP Base con cámara.

## IntercomUNICADOR

### Intercomunicador IP Modular

#### El intercomunicador deberá cumplir o superar las siguientes especificaciones de diseño:

##### El intercomunicador deberá incluir un servidor web integrado.

##### El intercomunicador deberá ser capaz de realizar funciones de control de acceso local definidas sin estar conectado a la red.

##### Le intercomunicador deberá tener soporte para la opción de incorporar una función de lector de RFID embebida.

#### El intercomunicador deberá cumplir o superar las siguientes especificaciones de funcionamiento:

##### Video

###### El intercomunicador deberá proporcionar transmisiones de video a una resolución de 640x480 a una tasa máxima de 30 imágenes por segundo usando formatos H.264, H.263, H.263+ o hasta 15 imágenes por segundo usando MJPEG.

###### La cámara del intercomunicador deberá suministrar imágenes en resoluciones de hasta 1280x960.

###### El intercomunicador deberá brindar soporte a los siguientes algoritmos de codificación de video:

H.263+

H.263

H.264

MPEG-4 Parte 2

MJPEG

###### El intercomunicador deberá proporcionar transmisiones simultáneas en H.264 y MJPEG configuradas independientemente.

###### El intercomunicador deberá soportar una Tasa de Bits Constante (CBR) en H.263, H.263, H.264 para proteger la red de picos inesperados de tasas de bits.

###### El intercomunicador deberá proporcionar niveles de compresión configurables.

###### Soporte para el perfil de base estándar H.264 con estimación de movimiento.

###### Soporte para estimación de movimiento en H.264/MPEG-4 Parte 10/AVC.

###### El intercomunicador debe permitir que el video se pueda transportar a través de:

HTTP (Unicast)

HTTPS (Unicast)

RTP (Unicast y Multicast)

RTP por RTSP (Unicast)

RTP por RTSP por HTTP (Unicast)

###### El intercomunicador deberá soportar *Quality of Service* (QoS) para poder priorizar el tráfico.

##### Imagen

###### La cámara deberá incorporar balance automático de blancos.

###### La cámara deberá soportar valores definidos manualmente para:

Niveles de color.

Brillo.

##### Audio

###### El intercomunicador deberá soportar audio bidireccional dúplex completo.

Fuentes de entrada

Un micrófono internos.

Fuentes de salida

Altavoz integrado, 2W

###### El intercomunicador deberá soportar niveles de volumen con ajustes por separado para:

Llamadas.

Teclas.

Tonos de llamada.

Clips de audio precargados.

Tonos de advertencia.

Comunicaciones.

###### El intercomunicador deberá soportar control adaptativo de la ganancia.

###### Codificación

El intercomunicador deberá soportar.

G.711

G.722 (banda ancha)

G.729

L16 / 16kHz (banda ancha)

###### El intercomunicador deberá suministrar un nivel de presión del sonido de al menos 78dB a 1kHz a 1m.

###### El intercomunicador deberá estar provisto de tecnología activa de cancelación de eco.

###### El intercomunicador deberá permitir que el audio se transporte por:

RTP (Unicast y Multicast)

RTP por RTSP (Unicast)

RTP por RTSP por HTTP (Unicast)

###### El intercomunicador deberá soportar *Quality of Service* (QoS) para poder priorizar el tráfico.

##### Función de llamadas

###### El intercomunicador deberá soportar SIP para su integración con VoIP, de pares o integrada en SIP/PBX.

###### El intercomunicador deberá soportar el uso de SIP Proxy, que puede ser el mismo registrador SIP para llamadas salientes.

###### El intercomunicador deberá soportar hacer llamadas hasta a doce números por separado de forma secuencial o como un mismo grupo de repique.

##### Función de control de acceso

###### Las salidas del intercomunicador deberán soportar el control remoto usando códigos DTMF.

###### Cada usuario tendrá códigos de acceso únicos para cada salida eléctrica.

##### Interfaz del usuario

###### Servidor web

El intercomunicador deberá contener una función integrada de creación de servidor web y configuración disponible para múltiples clientes en un entorno de sistema operativo y navegador estándar usando HTTP, sin necesidad de software adicional.

###### Especificación del idioma

El intercomunicador deberá proporcionar una función para modificar el idioma de la interfaz del usuario y deberá incluir soporte para un mínimo de 7 idiomas distintos, e incluir la capacidad de dar soporte a idiomas adicionales por medio de la personalización.

###### Direcciones IP

El intercomunicador deberá soportar direcciones IP tanto fijas como asignadas dinámicamente proporcionada por un servidor de Protocolo de Configuración Dinámica del Host (DHCP).

El intercomunicador deberá permitir su detección automática basada en WS Discovery cuando se utilice una computadora con un sistema operativo que soporte esta característica.

El intercomunicador deberá brindar soporte a IPv4.

##### Función de eventos

###### El intercomunicador deberá estar provisto con una función de eventos integrada, la cual podrá ser activada por:

Manipulación/apertura de la carcasa.

Estado de Llamada SIP, incluyendo llamada entrante.

Cambio del estado de registro SIP.

Detección de Movimiento en Video

Detección de Ruido

Secuencias DTMF sobre SIP

Entrada externa

Eventos de control de acceso, como tarjeta ingresada

Tiempo predefinido

###### La respuesta a los activadores incluirá:

Enviar una notificación, usando HTTP o correo electrónico.

Activar una alarma sonora.

Hacer o terminar una llamada.

Enviar una notificación usando HTTP, HTTPS, Wiegand o correo electrónico.

Enviar imágenes usando FTP o correo electrónico.

Activar salidas externas.

Reproducir clip de sonido.

##### Protocolo

###### El intercomunicador deberá incorporar soporte para, al menos, HTTP, HTTPS, SIP 2.0, TFTP, RTSP, RTP, SMTP, DHCP opt 66, NTP, Syslog.

###### La implementación de SMTP incluirá soporte para autenticación por SMTP.

###### La cámara deberá incorporar soporte para, al menos, HTTP, HTTPS, SIP 2.0, ICMP, SNMPv2c, RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, ARP, DNS, NTP,

##### Seguridad

###### El intercomunicador deberá soportar el uso de HTTPS y SSL/TLS, brindando la capacidad de cargar certificados firmados para encriptar y asegurar la autenticación y la comunicación tanto de los datos de administración y de las transmisiones de video.

###### El intercomunicador deberá bloquear su página de inicio de sesión por 30 segundos luego de que se hayan ingresado contraseñas incorrectas en tres ocasiones.

###### El intercomunicador deberá obligar a los usuarios a cambiar la contraseña de administrador luego de la primera instalación.

###### El intercomunicador deberá brindar una administración centralizada de certificados, con la capacidad de cargar certificados CA. Los certificados deberán estar firmados por una organización que proporcione servicios de confianza digital.

###### El intercomunicador deberá soportar la autenticación IEEE 802.1X.

###### Algunos servicios selectos, como RTSP o configuración web, deberán ser configurables para únicamente permitir el acceso desde dispositivos locales.

###### El intercomunicador deberá restringir el acceso al servidor integrado por medio de nombre de usuario y contraseña.

###### El intercomunicador deberá incluir un sistema de detección de manipulaciones.

##### Soporte de API

###### El intercomunicador deberá estar completamente soportado por una API (Interfaz de Programación de Aplicaciones) abierta y publicada, la cual deberá brindar la información necesaria para la integración de las funciones con aplicaciones de terceros.

###### El intercomunicador deberá cumplir con el estándar ONVIF, perfil S según lo define la Organización ONVIF.

Consulte las especificaciones del perfil ONVIF en el sitio web www.onvif.org/

###### El intercomunicador deberá ser interoperable/certificado con los fabricantes principales de PBX y puertas de enlace, incluyendo:

Cisco

Avaya

Broadsoft

##### Instalación y mantenimiento

###### El intercomunicador deberá soportar la configuración segura usando HTTPS.

###### El intercomunicador deberá soportar el uso de herramientas de gestión basadas en SNMP según SNMP v2c.

###### El intercomunicador deberá permitir las actualizaciones del software (firmware) por la red, usando TFTP, HTTP o una interfaz web.

###### El intercomunicador deberá aceptar sincronización horaria externa de un servidor NTP (Protocolo de Tiempo de Red).

###### El intercomunicador deberá soportar el respaldo y la restauración de la configuración.

###### El intercomunicador deberá almacenar todos los ajustes específicos del usuario en una memoria no volátil que no se perderá durante apagones o reinicios.

##### Registro de acceso

###### El intercomunicador deberá ser capaz de crear un registro de eventos, como códigos, llamadas telefónicas, tarjetas RFID, etc., y proporcionarlos usando una interfaz HTTP para el monitoreo.

###### El administrador deberá ser capaz de definir si se enviarán mensajes particulares por el intercomunicador inmediatamente después de que ocurra un evento, o si el cliente se registra para el seguimiento de eventos y luego solicita el informe completo desde el último registro, todos los eventos a la vez.

###### El cliente deberá ser capaz de seleccionar cuáles mensajes del registro de acceso se reportan.

##### Diagnósticos del intercomunicador

###### El intercomunicador deberá incluir LEDs capaces de proporcionar información de estado visible. Los LEDs deberán indicar el estado operativo del intercomunicador y brindar información acerca de energía, el estado de la red y el estado del dispositivo.

###### El intercomunicador deberá ser monitoreado por una función Guardián (*Watchdog*) que reiniciará automáticamente los procesos o reiniciará la unidad si se detecta un fallo de funcionamiento.

##### Interfaces de hardware

###### Interfaz de red

El intercomunicador deberá estar provisto de un puerto de Ethernet rápido 10BASE-T/100BASE-TX, usando un conector estándar RJ45 y deberá soportar la negociación automática de la velocidad de la red (100 MBit/s y 10 MBit/s) y el modo de transferencia (completo y semi-dúplex).

###### Puertas

El intercomunicador deberá estar provisto de una entrada programable que soporte ambas activaciones de cortocircuitos o hasta +30VDC para el monitoreo de puertas o Solicitud para Salir (REX, por sus siglas en inglés).

El intercomunicador deberá estar provisto de dos salidas independientes para el control de la puerta. Una activa que suministre al menos 8VDC / 600mA y un relé NO/NC que soporte hasta 30V AC/DC 1A.

###### Alimentación

El intercomunicador deberá tener un bloque terminal removible que proporcione la conectividad para una alimentación externa.

##### Carcasa

###### El intercomunicador deberá:

Fabricarse con una carcasa de categoría IP65, y tener una certificación IK07

Incluir un interruptor de seguridad.

Estar disponible con un acabado superficial negro.

##### Alimentación

###### Power over Ethernet IEEE 802.3af/802.3at Tipo 1 Clase 0

###### 12 V DC

Máx.: 2A

##### Ambiental

###### El intercomunicador deberá:

Operar en un rango de temperatura de -40 °C a +55 °C (-40 °F a 131 °F)

Operar en un rango de humedad de 10–95% HR (sin condensación).

# EJECUCIÓN

## INSTALACIÓN

### El Contratista deberá seguir cuidadosamente las instrucciones descritas en la documentación suministrada por el fabricante para asegurarse de que ha tomado todos los pasos necesarios para suministrar un sistema confiable y fácil de operar.

### Todos los equipos deben ser probados y configurados antes de la instalación, de conformidad con las instrucciones suministradas por el fabricante.

### Todos los firmwares de los productos deberán ser las últimas versiones, las más actualizadas que ofrezca el fabricante.

### Todos los equipos que requieran que los usuarios inicien sesión usando una contraseña serán configurados con contraseña(s) específicas para el usuario/sitio. No se permitirá mantener contraseñas por defecto del sistema o los productos.

FIN DE LA SECCIÓN