

TEMARIO DE TRABAJO

De los muchos temas que podrían tratarse en este tema de trabajo, se definen como prioritarios los siguientes, que extractamos:

- Sistemas de seguridad
 - ✓ integridad o parcelación del sistema
 - ✓ diseño del sistema
 - ⊕ proporcionalidad, densidad y adecuación
 - ✓ proyecto de seguridad
 - ⊕ contenido y requisitos formales
 - ✓ Violabilidad y fiabilidad de los sistemas
 - ⊕ vulnerabilidad técnica y cobertura
 - ✓ equipos de seguridad
 - ⊕ características exigibles
 - ⊕ protocolos de homologación
 - ⊕ información exigible
 - ✓ implantación de los sistemas
 - ⊕ formación al usuario e información
 - ⊕ manejabilidad
 - ✓ integración con reglamentos técnicos

- Alarmas
 - ✓ definición y tipología
 - ⊕ casuística y estadística
 - ✓ tratamiento y verificación por las CRA
 - ⊕ equipamientos y técnicas de verificación
 - ⊕ protocolos de actuación

- Mantenimiento de sistemas
 - ⊕ periodicidad y modalidades
 - ⊕ libro de revisiones
 - ⊕ renovación de equipos

- Personal técnico y operarios de CRA
 - ⊕ formación
 - ⊕ requisitos formales

En aras de la practicidad en el trabajo se decide agrupar los puntos anteriores en 5 grandes temas, desarrollados por una asociación y posteriormente revisados y completados en trabajo conjunto:

Tema de estudio por Asociación

PROTOCOLO DE CRA (AES)

VERIFICACIÓN TÉCNICA (FES)

MATRIZ DE DISEÑO DE SISTEMAS (ACAES)

PROYECTO- NORMALIZACIÓN, CERTIFICACIÓN (TECNIFUEGO)

MANTENIMIENTO (AMPES)

INTRODUCCIÓN

La Mesa de tecnología se constituye por las Asociaciones Empresariales del sector de seguridad: ACAES - AES - AMPES- FES - TECNIFUEGO/AESPI y las organizaciones sindicales UGT - CCOO.

Se inician las reuniones en la sede de ACAES en BARCELONA 19 de Mayo 2003, con reuniones posteriores en 2 de Junio, 16 de junio y sesiones finales 17 y 18 de julio. Revisión final de redactado de conclusiones el 24 de Septiembre.

El objetivo de la Mesa es describir y reconocer la situación en que se encuentra en la actualidad, el subsector de los sistemas de seguridad; su problemática específica, su evolución esperada, así como la configuración de un marco de trabajo deseable y sostenible.

Finalmente estos trabajos serán elevados al público conocimiento, complementando el resto de trabajos que configurarán el Congreso Nacional de Seguridad a celebre el próximo mes de Octubre, y serán base de la ponencia que en el mismo representará a los componentes de la Mesa.

CONCLUSIONES

De los trabajos presentados obtenemos las conclusiones siguientes:

- ❖ Los sistemas de seguridad persiguen un fin primordial que es la detección de intrusiones o presencia de personas no autorizadas dentro el ámbito de protección, lo que genera un aviso de alarma por medios ópticos/acústicos locales, o/y preferentemente, la transmisión codificada a una Central Receptora de Alarmas que la verifica y transmite a las fuerzas de Policía.
- ❖ Los prerequisites ideales de un sistema de seguridad se resumen en dos situaciones básicas:
 - ✓ Toda intrusión debe ser detectada y comunicada.
 - ✓ Toda transmisión de alarma derivada de un supuesto acto delictivo, debe de responder a un evento cierto susceptible de intervención policial.

Estos dos elementos básicos no agotan las posibilidades del sistema de seguridad, que puede englobar variado tipo de situaciones de origen antisocial (asalto, atraco, coacciones, sabotajes, hurtos, vandalismo, etc.) o de riesgos que pueden atentar contra la vida o la integridad de los bienes (fuego, inundación, fugas tóxicas, etc.) mas un sin fin de parámetros informativos que pueden ser útiles a efectos de una gestión integral de la seguridad, entre los que claramente debemos de situar los de control de imágenes por televisión, los de control de accesos y presencia, o los de seguimiento y posicionamiento de objetos o personas itinerantes.

Este enfoque permite valorar en su verdadera dimensión, la importancia de los sistemas de seguridad, que trasciende más allá de la consideración de meras alarmas, y cuyo fallo operativo o conceptual, si supone la posibilidad de afectación de vidas humanas, aparte de las posibles pérdidas materiales.

- ❖ Todo ello con el condicionante de que el sistema se configure de forma comprensible y de sencillo manejo para el usuario, integrable dentro del espacio arquitectónico, compatible con usos y costumbres del entorno, no accidental ni incidental, inmune a interferencias o condiciones naturales que puedan afectar su normal actividad, con capacidad de funcionamiento ininterrumpido 24 horas al día en circunstancias adversas y en equilibrio de coste eficacia con los riesgos que protege. Riesgos y amenazas que son generados principalmente por voluntad dolosa humana, con capacidad de análisis, planificación y aplicación de técnicas criminales para vulnerar y violar los sistemas, dentro de su propia ecuación de rentabilidad; que contempla la esperanza del botín, contrapuesta al esfuerzo (instrumental y humano) a emplear y al riesgo de ser capturado.
- ❖ Para conjugar los dos objetivos básicos se precisa profundizar en el origen de los problemas cuyas grandes líneas coinciden con los enunciados de los trabajos de la Mesa.

ASÍ, UNA BUENA INSTALACIÓN DE SEGURIDAD, ES AQUELLA QUE:

- ❖ **UTILIZA EQUIPOS HOMOLOGADOS POR UNA NORMA CUYA TECNOLOGÍA PRESENTE:**
 - ✓ Una tasa tendiendo a cero de causas espurias que pueden provocar un disparo del sistema.
 - ✓ Unos parámetros de detección, que sean difícilmente vulnerables o violables por pautas de comportamiento evasivas del intruso escalonadas en un gradiente proporcional a la focalización del riesgo, y correlativas a la definición de niveles técnicos de calidad (4) de la norma EN.
 - ✓ Terminales de comando con información suficiente para el usuario, y de fácil manejo.
 - ✓ Una duración media de funcionamiento óptimo conocida.
 - ✓ Estabilidad de funcionamiento seguro en ambientes y situaciones adversas.
 - ✓ Validación técnica testada.

Estas definiciones constituyen el trabajo desarrollado y a completar dentro del apartado de normalización y certificación, con una propuesta orientativa alternativa, para trasladar a la mesa del ámbito jurídico, de normalización de empresas instaladoras, siguiendo la pauta del sector de incendios y otras directrices que se vienen gestando en departamentos de Industria. Incluye la normativa EN aplicable.

- ❖ **ESTÁ DISEÑADA Y PROYECTADA POR EMPRESAS AUTORIZADAS DE SEGURIDAD**
 - ✓ Con un número de equipos y tipología de los mismos, capaz de cubrir el espacio a proteger con la densidad de detectores en número suficiente y ubicación adecuada para evitar la comisión del hecho criminal, sin ser detectado.

El número de equipos será proporcional a la configuración arquitectónica y accesibilidad del inmueble - situación y distribución de los bienes - factores de riesgo concurrentes (geográficos, ambientales...), factores psicológicos, modales, focalización criminal y al valor de los bienes (materiales, industriales, procedimentales, humanos) protegidos,

La densidad en la red de diseño, se considera como un método eficaz complementario para la verificación de la alarma y su transmisibilidad a la Policía.

- ✓ Con una configuración de detección que tenga en cuenta la ecuación: tiempo; detección; verificación; comunicación; respuesta.
- ✓ Dentro de un equilibrio coste / eficacia, que vendrá medido por una matriz funcional dinámica a largo plazo que ajuste la pérdida estadística evitada, contra el daño remanente y con la inversión necesaria que incluye sus coste de mantenimiento en el mismo plazo de tiempo comparado (generalmente de 4 a 10 años).

El cometido de análisis y diseño es sin duda responsabilidad de la empresa, y debería ser elaborado por un analista.

El objetivo es conseguir una herramienta práctica,- como guía, o pauta;- interpolable a un sistema de disposiciones normativas o de consenso, que permita el cálculo (en similitud con el caso de la protección de fuego) de equipos necesarios a utilizar en una instalación de seguridad, de acuerdo con los factores y variables que se introduzcan en el modelo.

Es potestad del cliente decidir su gasto o inversión en seguridad. Pero sin duda, para ejercer ese derecho debe de tener una información precisa, profesional y verosímil sobre el grado de cobertura y de la tipología de eventos de riesgo que abarca o cubre cada opción que se le ofrece. (Lo que inversamente significa: el grado de desprotección que está dispuesto a asumir en cada caso)

Esto implica establecer previamente como SECTOR, unas reglas de juego convenciones o normas claras, que supongan un cauce abierto, no una losa o corsé, suficientemente ágil para adaptarse a los cambios de la tecnología o cualesquiera otros y que dignifique una actividad global tan sensible como esta de seguridad, sin dejar por ello de ser Empresa, y como tal; actividad económica sujeta a las leyes de la competencia y del mercado.

Se trata en definitiva, ofrecer las mismas garantías a nuestros clientes, que nosotros estamos dispuestos a exigir a sectores tales como el de la sanidad, la alimentación, el tecnológico, el farmacéutico...etc.

Si una norma, guía, código o como quiera pueda llamarse, conviene que sea hecha. Mejor que sea hecha por los profesionales representados por las asociaciones de seguridad.

Las relaciones funcionales entre parámetros y vectores es parte del estudio de la Matriz de Diseño.

Se adjunta una tabla con cálculos paramétricos, como borrador de análisis y partida, para que el propio sector pueda proponer los cambios vectoriales y matemáticos que permitan el enriquecimiento de la misma, hasta conseguir un nivel general de aceptación y eficiencia.

❖ ES REALIZADA Y MANTENIDA CORRECTIVA Y PREVENTIVAMENTE POR EMPRESAS AUTORIZADAS DE SEGURIDAD

- ✓ Con implantación en situación de pruebas, por el tiempo que se considere oportuno, hasta el funcionamiento estable de la instalación.

Cumplimentando un programa de entrega y formación de los usuarios contrastado y suficiente.

Queda abierta la discusión sobre la conveniencia de imponer normativamente o no, que la instalación sea realizada íntegramente por empresa de seguridad, o dejar libertad, para la subcontratación o realización directa por empresas-no-de-seguridad, de partes que impliquen alta especialización genérica o complementaria y no esencial a efectos de seguridad.

La orientación unánime que tuvo la Mesa fue, por defensa del sector, ratificar la realización íntegra por empresa de seguridad de las instalaciones de seguridad separables o independientes (con excepción de la obra civil y opcionabilidad del cableado), y apoyarse en otros sistemas existentes o habilitados externamente (especialmente redes de comunicaciones) , en caso de integración con sistemas multipropósito o multitarea, domótica, etc., Siempre que la integración posterior a equipos de centralización de gestión y comunicación de datos, se realice desde una central de seguridad autónoma y con equipos de detección instalados y mantenidos por empresa de seguridad.

No se trata de poner puertas de salida hacia las nuevas tecnologías, y por lo tanto es lógico y deseable conectar los equipos de seguridad mediante y a través de redes de domótica, cable estructurado, tendido eléctrico, inalámbrico, IP... o cualquier otro medio de comunicaciones. Pero si es posible, y valga el símil; procuraremos viajar dentro de la autopista común en nuestro propio vehículo.

- ✓ Con intervenciones personales de técnicos cualificados, en número de visitas de mantenimiento preventivo, proporcional a los vectores de riesgo y a la naturaleza de obligado cumplimiento o no de las instalaciones.

La habilitación, que implica formación previa y continua, y verificación formal de requisitos, es fuente de recelos, no por no estar de acuerdo en la premisa básica de la formación, sino por temor a que el proceso formal implique restricciones de oferta en el mercado laboral y más problemas a la hora de confeccionar plantillas.

- ✓ Complementadas con verificaciones bidireccionales de estado, que no podrán suplir totalmente el mantenimiento preventivo, aunque si espaciarlo en función del estado de la técnica aplicada y de las posibilidades reales de conocimiento de estado y eficacia de cobertura de los equipos detectores.

Hay una cierta disparidad, a la hora de considerar la asignación de periodos mínimos de mantenimiento. Por un lado, hay una apreciable diversidad en la tipología de las instalaciones, lo que obligaría a una clasificación muy precisa a la hora de redacción de cualquier texto normativo. . Por otro lado es evidente que los avances técnicos evolucionan más rápidamente que las posibilidades de corrección de la norma. Pero no hemos de equivocarnos: la evolución afecta automáticamente solo parte de las nuevas instalaciones con esas nuevas técnicas, no las anteriores y convencionales que coexisten durante bastante tiempo.

La consideración de la Mesa fue; que los mantenimientos preventivos presenciales, son necesarios (en número que será fijable y variante en función de la tecnología aplicada) no solo para prevenir averías, sino para ajustes y limpieza precisos, así como la comprobación de la idoneidad de ubicación y coberturas ante configuración cambiante del espacio protegido.

El mantenimiento preventivo es el mecanismo de perfeccionamiento progresivo de un sistema.

¿Porqué establecer un número fijo de 2, 4, 12 o ninguno? Puede ser una discusión casi filosófica... Contrariamente también podemos dejar la libre voluntad de las partes..

La tendencia por intereses económicos y a veces la ignorancia de ambas partes llevará a cero mantenimientos obligatorios, aunque se necesiten las máximas exigencias de buen funcionamiento. ¿Demuestra la historia del sector la compatibilidad natural de los dos objetivos?

Consecuentemente, la Mesa- unánimemente - estima, debe haber un número mínimo variable, en función de distintos parámetros expuestos (ambientales, riesgo, tecnología aplicada), precisamente como una medida de protección del propio usuario y por sanidad del sector.

- ✓ Con un programa preestablecido con el manual de manejo y conservación de la instalación, de renovación (recomendada o automática según criterios) de equipos al término de su vida estadística promedio útil sin averías.
- ✓ Con sistemas de transmisión que aseguren la recepción de las señales o su interceptación, en las Centrales Receptoras de Alarma habilitadas.

Las líneas fundamentales del mantenimiento están recogidas en el trabajo sobre mantenimiento.

- ❖ **ESTA CONEXIONADA POR MEDIOS DE TRANSMISIÓN CONSISTENTES CON UNA CENTRAL RECEPTORA DE ALARMAS HOMOLOGADA, QUE EFECTÚA LA RECEPCIÓN DE SEÑALES DE ALARMA Y DE ESTADO ASÍ COMO LA VERIFICACIÓN DE VEROSIMILITUD Y TRANSMISIBILIDAD A POLICÍA DE LAS MISMAS.**

- ✓ Mediante personal formado y capacitado, y en número proporcionado, no lineal, para una atención diligente, a la cantidad de instalaciones conexas, la estacionalidad y fluctuaciones horarias, y a los propios requisitos operativos de los equipos.

La capacitación, siguiendo el criterio establecido para el personal instalador, debe potenciarse sin que suponga un agravante de mercado laboral. Se estimula para que las propias asociaciones elaboren, potencien y controlen una programa formativo

- ✓ Con los medios técnicos que el estado de la tecnología permita en cada momento.
- ✓ Siguiendo Protocolos de Verificación y toma de decisiones preestablecidos en función de los dispositivos técnicos implementados en cada usuario, (*bidireccional, telefónica, visual, acústica, secuencial, presencial, etc.*) y de la propia información codificada recibida en orden de secuenciación o redundancia programada.

Dentro del mandato imperativo de hacer mínima la cadena de tiempos: detección-verificación-comunicación- reacción

- ✓ Las Centrales receptoras deben, además de realizar las gestiones de señales de tratamiento "policia", recibir aquellas otras de tipo visual, fónico, paramétrico o de control que sean consustanciales con las amplias posibilidades y necesidades de los sistemas de seguridad en su visión integral.

Las líneas principales están desarrolladas en el PROTOCOLO DE VERIFICACIÓN

Este conjunto de medidas elaboradas e implementadas con una visión integral, sin duda, coadyuvaran a la consecución del segundo objetivo enunciado y deseado por todos; La reducción de las alarmas no susceptibles de tratamiento policia, y su transmisión a la policia.

PARA ELLO VOLVEMOS AL ORIGEN.

La tipificación y cómputo estadístico de las señales de alarma, nos revelan la eficacia de las distintas medidas de acción enunciadas o la necesidad de otras acciones o soluciones complementarias.

- ❖ Soluciones para **manipulaciones indebidas** (60 a 80%)
 - ✓ Por falta de formación adecuada de inicio
 - ✗ obligación de entrega de manuales prácticos, entendibles y acto de entrega con tiempo suficiente, firmado por usuarios.
 - ✗ Prontuarios impresos en elementos de control del sistema
 - ✓ Por dificultad de manejo
 - ✗ valoración de la sencillez de manejo dentro de los parámetros homologables

- ✓ Por desconocimiento de usuarios devenidos, por manejo esporádico, por olvido, por negligencia
 - ✗ es obligación del usuario principal; debe de responsabilizarse al mismo de este hecho
 - ✗ obligatoriedad de la empresa instaladora sobre la instrucción a solicitud del usuario. (como servicio remunerado).

- ✓ Por sistemas de conexión que no dan información adecuada
 - ✗ es la problemática entre la comodidad y la seguridad.
 - ✗ No homologar sistemas de conexión o manejo que no den información al cliente de las anomalías que impiden la correcta conexión o real situación de conexión

- ❖ Soluciones para **causa espurias** (10%)
 - ✓ Calidad técnica ante interferencia.
 - ✓ Parámetros de homologación.
 - ✓ Ubicación inadecuada de equipos ?diseño.
Poner equipos adecuados, en número suficiente, en los lugares idóneos
 - ✓ Utilización de equipos inapropiados ? diseño; responsabilidad de la empresa instaladora sobre el proyecto.

- ❖ Soluciones para **averías** (10%)
 - ✓ Fijar el máximo aceptable. Cero es imposible. Todo se avería
 - ✗ Mayor correlación con bidireccionalidad
 - ✗ Densidad de equipos permite desconexiones temporales de elementos sin merma de eficacia.
 - ✗ Redundancia y secuenciación
 - ✗ diseño

 - ✓ Calidad técnica de equipos
 - ✗ Parámetros de homologación y correspondencia de los niveles de fiabilidad y vulnerabilidad de los equipos con el nivel técnica de la amenaza y el riesgo.
 - ✗ Mantenimiento correctivo contratado obligatorio en todo caso

 - ✓ Mantenimiento preventivo correlativo a riesgo de avería en todo caso
 - ✗ Implementar el plan voluntario de renovación automática preventiva de equipos al término de su vida óptima, antes de averías.
 - ✗ Vectores que suponen mayor necesidad de mantenimiento :
 - ✗ Incremental por número de equipos: No proporcional
La densidad de equipos no supone causa de incremento de frecuencia en visitas preventivas, considerándose que al contrario, permite la eficacia de los sistemas, aun cuando se provoque la desconexión temporal de un elemento hasta la subsanación correctiva. Sería injusto incrementar proporcionalmente este concepto. Por otro lado si el incremento de equipos viene motivado por una configuración solapada, la avería de un equipo tendrá pocas consecuencias tanto para la emisión de falsas alarmas a la central receptora, tanto como para la continuidad en la eficacia de detección.

- ✘ Equipos perimetrales y de exteriores - recomendado, coeficiente incremental, de 2 a 4 veces sobre mínimo de revisiones en función de la técnica y riesgo
- ✘ Equipos en ambientes polucionantes o inestables- recomendado , de 2 a 4 veces sobre mínimo de revisiones -en función de la técnica y riesgo

- ✘ Obligado cumplimiento - 1.5 a 3 veces sobre mínimo de revisiones - en función posibilidades reales comprobación bidireccional. El incremento en estos casos no viene solo por la prevención de averías técnicas, sino por evitación averías funcionales y sobre todo ajuste de coberturas
- ✘ Antigüedad - proporcionalmente creciente al exceso sobre supuesta vida límite si no se aplica plan de renovación,

Verificación técnica - la central receptora

❖ ¿Que se puede hacer? Se está realizando la carga de la prueba sobre la verificación por CRA, cuando en realidad esta tiene pocas cosas reales que hacer en las instalaciones de diseño insuficiente. Ya está demostrado que la bidireccionalidad por si sola, no es un medio consistente de verificación; Si, de programación, y conocimiento de estado, así como complemento de verificación en algunos sistemas por rearme de zonas. Adicionalmente, hay un gran parque de instalaciones que no son o no se pueden considerar bidireccionales, aun cuando tengan unidad de control o centralita bidireccional *Drásticamente podría impedirse la conexión a Central Receptora, de ningún sistema que no tuviera elementos técnicos de verificación... Quedarían un pequeño % de conexiones.*

❖ Posibilidades:

- ✘ Conexionar solo sistemas con numero suficiente de detectores para exigir la activación de grupos o secuencias lógicas no solucionaríamos los casos de animales en la zona o intrusión del propio abonado negligente. ¿ ¿ Sería causa de desconexión la primera hasta subsanación y de sanción o tasa para el usuario la segunda

- ✘ Conexionar solo instalaciones con capacidad de envío de señal de conexión y desconexión.

No considerar alarma las ocurridas, inmediatamente antes o inmediatamente después de la conexión con código.

Queda latente el riesgo de intrusión con coacción, u oportunista (intrusión inmediata tras salida usuario).

La primera se soluciona con los códigos de alarma silenciosa,

La segunda ¿? ... Habría que convenir en considerar alarma real la que provoca la activación de otros detectores además de los de entrada/salida. Mas la atención al posible corte de línea inmediatamente después.

Comprobar línea de comunicación, bien bidireccionalmente bien por "test" programado ¿ La manipulación indebida corregirla con tasas o desconexiones temporales o definitivas del abonado ¿?

- ❖ La verificación fónica es operativa en ámbitos restringidos y determinados.
 - ✓ No todas las intrusiones originan ruidos reconocibles.
 - ✓ La línea telefónica, puede estar siendo utilizada por el propio sistema de alarma.
La línea interrumpida, ¿está ocupada, cortada o es un fallo operativo?
 - ✓ Hay ruidos de fondo que pueden conducir a error. Ej. Ladridos de perro atado o encerrado en estancias contiguas, contra el ladrón. ¿se tomará por un perro suelto que ha causado una falsa alarma?
- ❖ La verificación por televisión tiene restricciones por número y también por cuestiones de privacidad. Será principalmente utilizable en ciertos ámbitos sectoriales de tipo comercial o industrial.

Así todo, la comprobación de una presencia, no implica la veracidad de delito a efectos policiales. los operarios de una CRA no conocen al usuario o allegados en actuación negligente.

La negligencia, que hasta ahora se contabiliza como manipulación indebida, debe de ser considerada como alarma real y compensarse con tasas de servicio cobrada al usuario responsable de la misma.

- ❖ Cualquier sistema de verificación desde CRA implica la utilización de canales y redes de comunicación, generalmente pensados para uso comercial sin formato de riesgo. Esto ofrece una cierta facilidad para el ataque de las mismas, sin certidumbre de que la pérdida de conexión sea indicativa de sabotaje, dada la frecuencia de fallos de los propios sistemas.

Sin una red de transmisión bidireccional segura, todo el desarrollo en diseño y tecnología de detección se viene abajo.

Es imprescindible un esfuerzo del sector en su totalidad para forzar la aplicación de soluciones seguras, o bien buscar alternativas propias - se podría hablar de un satélite, o contratación de redes exclusivas- para la transmisión de señales de seguridad que presentaran el nivel de funcionamiento continuado y No- Violabilidad que el tema requiere.

En este caso como en otros se revela claramente la conveniencia de un sector fuerte y cohesionado, con capacidad para realizar acciones conjuntas o incluso de normalización y homologación, sin necesidad de depender de la lógica rigidez de la administración. Un tipo de Unión o Colegio, es posible sin la pérdida de la personalidad de las Asociaciones actuales.

- ❖ Imparablemente la tecnología evoluciona a pasos agigantados y va entregando nuevas soluciones a las que debemos de permanecer abiertos. Nuevos campos, paralelos a la seguridad, se abren ante nosotros como la domótica y la globalización de las comunicaciones, que suponen enormes posibilidades y nuevos retos.

- ❖ Es ley, que cada nueva solución lleva incorporada su propia vulnerabilidad, lo que implica continuos esfuerzos de análisis y mejoras

Nada garantiza la supervivencia y estabilidad a niveles altos, de ningún sector económico, excepto el acierto en las decisiones individuales y colectivas de los profesionales que ocupan ese sector con visión a largo plazo.

No se trata de poner trabas a las salidas, sino condiciones adecuadas de entrada. Tampoco de oponerse a ningún sistema comercial, grande o pequeño, ni mucho menos de limitar posibilidades de competencia. Solo fijar los mínimos que permitan un crecimiento sostenido y armónico del SECTOR ofreciendo al usuario las máximas garantías de calidad y eficacia.

- ❖ Un buen consenso implica muchas horas de trabajo y esfuerzos de todas las partes

SI HAY QUE HACER LAS COSAS BIEN; ¡HAGÁMOSLO NOSOTROS!