

Política del Sistema de Gestión Integrado

cuyos alcances son:

ISO 9001 ISO 14001 ISO 45001	Instalación y mantenimiento sistemas de seguridad. Instalación y mantenimiento de sistemas contra incendios: • Sistemas de detección y de alarma de incendios. • Sistemas de señalización luminiscente, alumbrado de emergencia.	ISO 27001	Sistema de gestión de seguridad de la información que soporta los servicios de: • Soporte informático prestados por el Dpto. de Informática a todos los departamentos a nivel nacional e Internacional • Protección de Materias Clasificadas • Asesoramiento y Desarrollo Integral de proyectos de seguridad • Planificación, Control y Ejecución de obras de instalaciones y mantenimiento de Sistemas de Seguridad y Protección Contra incendios
ISO 22301	Instalación y mantenimiento de sistemas de seguridad Instalación y mantenimiento de sistemas contraincendios: • Sistemas de hidrantes contra incendios. • Extintores de incendio. • Sistemas de bocas de incendio equipadas. • Sistemas de columna seca. • Sistemas fijos de extinción por rociadores automáticos y agua pulverizada. • Sistemas de protección contra incendios que empleen gases fluorados como agente extintor.		• Sistemas fijos de extinción por agua nebulizada. • Sistemas fijos de extinción por espuma física. • Sistemas fijos de extinción por polvo. • Sistemas fijos de extinción por agentes extintores gaseosos. • Sistemas fijos de extinción por aerosoles condensados. • Sistemas para el control de humos y de calor. • Mantas ignífugas. • Sistemas de abastecimiento de agua contra incendios.
ISO 20000-1	A. El Sistema de Gestión de Servicios de TI soporta la prestación de los servicios de las instalaciones/Mantenimiento de Sistemas de Seguridad Electrónica gestionando: - Protección de materias clasificadas. - Asesoramiento y desarrollo integral de proyectos de seguridad. - Planificación, control, ejecución, instalación, mantenimiento y soporte de sistemas de seguridad electrónica y de protección contra incendios. - Soporte informático y gestión de las infraestructuras de TI, redes y centros de procesamiento de datos. - Ciberseguridad, seguridad de la información, inteligencia de amenazas y continuidad de los servicios de los sistemas de seguridad Electrónica; - Asesoramiento estratégico en seguridad; - Desarrollo, ingeniería, mantenimiento y soporte de sistemas de seguridad.		

Las intenciones de SAIMA SEGURIDAD en materia de gestión de los sistemas implantados son las indicadas en el Manual de Gestión en el Apartados 3.3 Política, que son:

- Cumplir con los requisitos de los clientes, así como con los requisitos legales y reglamentarios de aplicación.
- Desarrollar y poner en el mercado productos fiables y robustos, con reducido impacto ambiental desde una perspectiva de ciclo de vida.
- Trabajar con productos líderes en el mercado, descartando la utilización de productos cuya eficacia, fiabilidad y durabilidad no se encuentren suficientemente contrastadas.
- Ofrecer al cliente personal técnico de elevada cualificación, tanto por su formación como por su experiencia.
- Asegurar la capacidad de respuesta en el menor tiempo posible mediante el despliegue territorial de dotaciones móviles específicas para cada zona de actuación, y por medio de una organización adecuada en la recepción y valoración de los avisos de asistencia y en la utilización de los medios técnicos necesarios para la solución de las incidencias.
- Disponer de un soporte técnico de los fabricantes, en los productos principales, que asegure la solución de cualquier problema transmitido por el cliente.
- Prevenir la contaminación mediante:
 - La optimización de nuestros procesos productivos
 - El empleo de la mejor tecnología disponible a nuestro alcance
 - La gestión adecuada de los residuos generados
- Minimizar el consumo de recursos no renovables y reciclar los materiales en lo posible.
- Identificar los peligros y riesgos presentes en todas nuestras actividades y áreas de trabajo, notificarlos a nuestro personal junto con las medidas de prevención y control correspondientes, con el fin de eliminar o minimizar accidentes, lesiones y enfermedades laborales derivados de ellos.
- Proteger la salud y el bienestar laboral de nuestro personal, proporcionándoles un ambiente y condiciones de trabajo seguro, sano y saludable de acuerdo con las leyes aplicables.
- Consultar y asegurar la participación de los trabajadores en materia de seguridad y salud en el trabajo
- Establecimiento y cumplimiento de los requisitos contractuales con las partes interesadas.
- Tener como objetivo garantizar la confidencialidad, integridad y disponibilidad de los datos contenidos en los sistemas de la información de SAIMA.
- Prevención y detección de virus y otro software malicioso, mediante el desarrollo de políticas específicas y el establecimiento acuerdos contractuales con organizaciones especializadas.
- Gestión de la continuidad del negocio, desarrollando planes de continuidad conformes a metodologías de reconocido prestigio internacional.
- Realizar los preparativos necesarios y planificar un conjunto suficiente de procedimientos para responder de forma adecuada ante un incidente, desde el momento en que se declare el desastre hasta la vuelta a la normalidad, de forma que se reduzca al mínimo su impacto sobre el negocio, aumentando la confianza de nuestros clientes y otras partes interesadas.
- Proteger todos los recursos frente a amenazas internas o externas, deliberadas o accidentales.
- Establecimiento de las consecuencias de las violaciones de la política de seguridad, las cuales serán reflejadas en los contratos firmados con las partes interesadas, proveedores y subcontratistas.
- Actuar en todo momento dentro de la más estricta ética profesional.
- Establecer y revisar la política del Sistema de Gestión, siendo comunicada a toda la Organización a través del gestor documental usado en la organización y/o su publicación en paneles informativos, siendo revisada anualmente para su adecuación y extraordinariamente cuando concurren situaciones especiales y/o cambios sustanciales en el Sistema de Gestión, estando a disposición público en general.
- Mejorar continuamente la eficacia del sistema de gestión integrado, del Sistema de Gestión de Servicios (SGS) de TI y de los propios servicios prestados.
- Garantizar la alta disponibilidad, seguridad, continuidad y fiabilidad de nuestros servicios de TI, asegurando el estricto cumplimiento de los niveles de servicio acordados (SLA) con nuestros clientes y partes interesadas.

La dirección se asegura que: 1) el conjunto del personal es consciente de la importancia de la política de gestión; 2) la difusión de la política a las partes interesadas como dentro de la organización, mediante: charlas, comunicados, publicación en la página web de la empresa, etc.

