POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Aludium es una empresa líder en el sector del Aluminio, con una amplia gama de aplicaciones y productos para diferentes sectores como aplicaciones arquitectónicas, envases, energía y aislamiento, herramientas y dispositivos, así como distribución y automoción; Aludium cuenta con 3 plantas productivas en España y Francia y su centro de I&D-Cindal, aporta soluciones y productos con una amplia gama de aleaciones.

Para Aludium, la sostenibilidad es parte de nuestro ADN, por eso estamos desarrollando productos con una huella de carbono certificada, garantizando su trazabilidad desde la producción hasta su comercialización.

Por este motivo, ha implantado un **Sistema de Gestión de Seguridad de la Información**, cuyo objetivo es alcanzar la satisfacción esperada por los clientes a través de unos procesos establecidos y fundamentados en la mejora continua, garantizando la continuidad de los sistemas de información, minimizando riesgos y asegurando el cumplimiento de los objetivos fijados, para asegurar en todo momento la **confidencialidad, integridad** y **disponibilidad** de la información.

Para ello asumimos nuestro compromiso con la seguridad de la información, según las normas de referencia **TISAX**, para lo que la Dirección establece los siguientes principios:

- **Competencia y liderazgo** por parte de la Dirección como compromiso para desarrollar el sistema de Seguridad de la Información.

- Establecer **objetivos y metas** enfocados hacia la evaluación del desempeño en materia de seguridad, así como a la **mejora continua** en las actividades reguladas en el Sistema de Gestión de seguridad de la información.

- Cumplir los requisitos de la **legislación aplicable** a nuestra actividad, los compromisos adquiridos con los clientes y las partes interesadas, y todas aquellas normas internas o pautas de actuación a los que se someta la empresa.

- Asegurar la **confidencialidad** de los datos gestionados, la **integridad** y la **disponibilidad** de los sistemas de información y activos de información, tanto en los servicios ofrecidos a los clientes, como en la gestión interna, evitando alteraciones indebidas en la información.

- Asegurar la **capacidad de respuesta ante situaciones de emergencia,** restableciendo el funcionamiento de los servicios críticos en el menor tiempo posible.
- Establecer las medidas oportunas para **el tratamiento de los riesgos** derivados de la identificación y evaluación de activos.
- Garantizar un **análisis** continuo de todos los **procesos relevantes,** estableciendo las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

Para alcanzar estos objetivos generales la Dirección de esta empresa asume el firme compromiso de optimizar su política de seguridad de la información basada en los siguientes factores:

- **Prevención de Riesgos:** Establecer las directrices y medios necesarios en materia de prevención de riesgos con el objetivo fundamental de eliminarlos o mitigarlos
- **Compromiso con la protección del medio ambiente:** Reducir y prevenir los impactos medio ambientales generados por nuestras actividades, productos o servicios.
- **Requisitos Legales:** Entender los requisitos legales y otro tipo de requisitos especificados por nuestros clientes como un conjunto de mínimos a cumplir.
- **Difusión:** Difundir y promover la mejora de la seguridad de la información. La difusión efectiva de estas políticas es esencial para asegurar su cumplimiento y la protección de los activos de información.
- **Grupos de interés:** Participación conjunta con todos nuestros STAKEHOLDERS por una mejora de la seguridad de la información.
- **Capacitación:** Capacitación constante de todos nuestros profesionales, en conocimientos técnicos, y habilidades, fomentando su participación y compromiso con esta política, la mejora del sistema y la seguridad de la información.
- **Seguimiento**: Establecer indicadores a todos los niveles que nos permitan tomar decisiones basadas en la evidencia.
- **Mejora continua:** Establecer y revisar periódicamente objetivos y metas, que proporcionen un marco de referencia para la mejora continua de los procesos y del desarrollo sostenible.

- **Analizar:** Analiza y evaluar las desviaciones que puedan producirse en materia de seguridad de la información y establecer las acciones correctivas y oportunidades de mejora necesarias.

- **Sistema integrado:** Elaboración participativa de todos los grupos de la organización, a todos los niveles, siendo conscientes de la aportación a los objetivos del sistema y las repercusiones de los incumplimientos.

- **Consecuencia por incumplimiento:** El incumplimiento de las políticas de seguridad de la información puede tener graves repercusiones para la organización y sus empleados. Las violaciones de estas políticas serán tratadas con la máxima seriedad y pueden resultar en medidas disciplinarias, que van desde advertencias hasta la terminación del contrato de trabajo, según la gravedad de la infracción. Además, en caso de que el incumplimiento derive en consecuencias legales, los empleados pueden enfrentarse a sanciones civiles o penales.

- **Revisiones periódicas de la política:** Con el fin de garantizar que nuestras políticas de seguridad de la información se mantengan actualizadas y efectivas, se llevarán a cabo revisiones anuales. Estas revisiones considerarán los cambios en la normativa, la evolución de las amenazas de seguridad y las modificaciones en la estrategia de la organización. Cuando sea necesario, las políticas serán ajustadas para reflejar nuevas realidades y garantizar su alineación continua con las mejores prácticas del sector.

Estos principios son asumidos por la Dirección, que dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándose y poniéndolos en público conocimiento a través de la presente Política de Calidad y Seguridad de la Información.

La Gerencia de Aludium