

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

Nuestra meta

Los activos y la información de **CYMI** y sus empresas filiales y sucursales son esenciales para mantener su posicionamiento de liderazgo y referencia en los mercados en que están presentes, así como para la toma de decisiones a nivel estratégico. Nuestra meta consiste en asegurar la protección de las personas, los bienes, los derechos de propiedad industrial, intelectual e internet, los secretos empresariales, el conocimiento (know how) y la información, así como las operaciones e intereses de la Compañía, frente a agresiones y malas prácticas internas y externas de cualquier origen, físico o digital, prestando especial atención a los activos estratégicos y fomentando una cultura de seguridad, al amparo de los valores del **Grupo CYMI**.

Para alcanzar esta meta, se define esta política cuyo propósito es establecer un marco para la gestión de la seguridad de la información de manera que ninguna situación de emergencia, producción o resultado económico, pueda comprometer la **integridad, confidencialidad, trazabilidad, autenticidad o disponibilidad** de la información y de los servicios prestados.

Nuestros compromisos

Cumplimiento de la legislación vigente: Asegurar el cumplimiento de los requisitos legales en materia de protección de la información en cada ubicación y país donde operamos.

Normativa interna: Desarrollar la normativa interna necesaria que establezca estándares de comportamiento, promoviendo la difusión de los criterios de protección de activos y creando un marco común de actuación coherentes con las directrices definidas en el presente documento, y con la Política y Guías de Ciberseguridad marcadas por el **Grupo VINCI**.

Respeto a los activos de terceros: Respetar la información de terceros, incluyendo la confidencialidad y los derechos legítimos de propiedad industrial, intelectual y secretos empresariales, así como garantizar el respeto a nuestros propios activos e información.

Provisión de recursos Proveer recursos adecuados para la protección y salvaguarda de personas, intereses, bienes, operaciones, conocimientos, derechos de propiedad industrial, intelectual e internet, secretos empresariales e información del Grupo, así como los activos que los soportan. Implementar soluciones tecnológicas y procesos para evitar el uso incorrecto de las tecnologías de la información.

Conciencia de protección de activos: Realizar actividades de formación y divulgación entre los empleados sobre la protección de activos, para que velen tanto por su propia seguridad como por la de los activos de la Compañía en sus respectivos ámbitos de responsabilidad.

Gestión basada en análisis de riesgos: Llevar a cabo estudios de protección de activos en las diferentes Unidades de Negocio/Áreas Corporativas, con el objetivo de identificar adecuadamente los riesgos y adoptar medidas para gestionarlos.

Coordinación de la información: Establecer y mantener canales de información interna y externa que permitan conocer la situación de protección de activos.

Mejora continua: Establecer objetivos de mejora y metas de protección de activos de manera sistemática, evaluando el desempeño y aplicando las correcciones necesarias para alcanzar los logros propuestos, definiendo procesos de verificación, auditoría y control para asegurarlos.