POLÍTICA DE CIBERSEGURIDAD

En ERMUA a 26 de junio de 2026

ECS Mobility es una empresa especializada en la fabricación de coronas de arranque y aros para el mercado del sector Automoción.

Actualmente la información y el know-how son dos de los recursos más importantes para ECS y garantes de su viabilidad por lo que consideramos un compromiso fundamental la protección de dicha información y los activos que la sustentan, garantizando la confidencialidad, integridad y disponibilidad de los activos y procesos digitales de la Organización.

A raíz del acelerado proceso de digitalización y del consiguiente aumento de ciberataques por parte de *hackers* de todo el mundo en ECS se considera la ciberseguridad como un **aspecto prioritario.**

La Dirección de la empresa, tras evaluar el valor de sus activos y los riesgos a los que están expuestos, apoyándose en los tres pilares que se indican a continuación establece una serie de directrices de seguridad de la información comprometiéndose a proporcionar los recursos necesarios para desarrollar las decisiones o medidas a tomar respecto a la **seguridad de sus sistemas de información**.

Los tres pilares que soportan esta política son:

- **Identificación** precisa del **capital digital** de ECS para una adecuada toma de decisión de quiénes serán los responsables de gestionar los riesgos de seguridad de tecnología de información.
- Fomento de una **cultura de ciberseguridad** que involucre a todo el personal desde los directivos hasta el último empleado.
- **Plan de formación** para todos los trabajadores expuestos a ciber-riesgos de la mano de la concienciación ante posibles ciber-amenazas e incluso efectuando simulacros de ciberataques.

Considerando los riesgos asociados a la ciberseguridad a los que está expuesta la organización la Dirección se compromete a implantar las medidas necesarias, por lo que asume los siguientes **compromisos**:

- **Evaluar por anticipado** los posibles riesgos en materia de ciberseguridad en nuestras actividades y operaciones, adoptando las medidas de gestión que se consideren necesarias en función de su nivel de riesgo.
- Ofrecer el **nivel apropiado de ciberseguridad** durante el desarrollo de las actividades y operaciones, tanto a nuestros empleados como de nuestros activos y procesos.
- Asegurar la completa **integración de los compromisos de ciberseguridad** con nuestros grupos de interés en todos los sistemas de gestión proporcionando las estructuras y recursos para poner en marcha las iniciativas necesarias.
- Garantizar que todos los empleados son debidamente **informados y capacitados** en materia de ciberseguridad con el fin de tener presentes las prácticas de trabajo y los procedimientos establecidos para el desempeño de sus funciones.
- Implantar sistemas de **monitorización, detección y alerta temprana** que permitan una identificación permanente y continuada de las vulnerabilidades, nuevas amenazas e incidentes a nivel global, así como definir los mecanismos oportunos para asegurar que las personas encargadas de la protección de nuestros activos, sus infraestructuras y/o de sus sistemas de información estén informados de dichas incidencias en forma y plazo.
- Establecer **procedimientos y responsabilidades** de respuesta inmediata, eficaz y ordenada ante incidentes de ciberseguridad, así como **planes de contingencia** específicos.

El papel de la Dirección de ECS Mobility es fundamental en la consecución del éxito de esta política y, con el objetivo de obtener una completa integración en la organización ya que incumbe a todos los miembros de la misma esta política se hace pública y accesible para todos sus empleados, clientes, proveedores y para el público en general manteniéndola al día mediante revisiones periódicas.

Rafael Barahona
CEO & Plant Manager

ECS Mobility