CIE Automotive

Política de tecnologías de la información y de riesgos de ciberseguridad

Contenido

El Consejo de Administración de CIE Automotive, S.A. (en adelante "**CIE Automotive**", la "**Sociedad**" o el grupo de sociedades del que CIE Automotive es la sociedad dominante, el "**Grupo**"), aprueba esta Política de tecnologías de la información y de riesgos de ciberseguridad, que forma parte de las políticas de gobierno corporativo y cumplimiento normativo y que recoge los principios y directrices que dan soporte a una adecuada gestión de la seguridad de la información.

1. Objeto

La presente Política de tecnologías de la información y de riesgos de ciberseguridad tiene como objetivo marcar los principios y directrices que den el soporte adecuado para una correcta gestión de la seguridad de la información, de modo que se asegure el adecuado control, rigor y cumplimiento en las actuaciones que se lleven a cabo.

CIE Automotive reconoce la importancia que tiene la seguridad de la información para la correcta realización de sus actividades.

Por ello ha desarrollado esta política que fija e integra los principios básicos de seguridad con los requisitos operativos en términos de confidencialidad, autenticidad, trazabilidad, integridad, disponibilidad y conservación de la información.

El principal objetivo de esta política es reforzar el compromiso de CIE Automotive con los empleados, empresas, clientes y proveedores, expresado en términos de mejora continua del servicio ofrecido, del cumplimiento de la legislación aplicable, de la mejora de los procesos internos y de la protección de la información manejada dentro del entorno de CIE Automotive.

Se hace por tanto necesario que todas las personas que interaccionen de manera directa o indirecta con CIE Automotive conozcan la política y normativas pertinentes y apliquen sus directrices como tareas propias de las funciones desarrolladas en su vinculación con la misma.

Así pues, la Política de tecnologías de la información y de riesgos de ciberseguridad desarrollada en este documento velará por garantizar la protección de los activos de información de CIE Automotive, siendo ésta de aplicación en todas las fases del ciclo de vida de dichos activos: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción.

Para la aplicación efectiva de la presente Política y de la Normativa que la desarrolla, CIE Automotive se dotará de los recursos necesarios para su buen desarrollo, tanto en lo referente a las actividades de implantación como de mantenimiento, incluyendo los controles o medidas de seguridad que en cada ámbito se establezcan.

2. Alcance

El alcance de la presente política comprende:

- ✓ A todas las sociedades que componen CIE Automotive.
- ✓ A contratistas y terceros con acceso a los activos de ambos, o bajo su responsabilidad.
- ✓ A la información tratada almacenada y custodiada desde cualquier área del grupo.
- ✓ A todas las instalaciones, recursos y procesos utilizados para la prestación de servicios, sean estos internos o vinculados con terceros a través de acuerdos o contratos.

Además, esta política persigue a realizar un seguimiento de la cadena de suministro para asegurarse de que sus compromisos están alineados con los de la sociedad, así como gestionar la seguridad de la información en el desarrollo y fabricación de los productos que comercializa.

Esta política se ubica dentro del marco jurídico definido por la legislación y normativa vigente, relacionada directa o indirectamente con el tratamiento de la información mediante métodos automatizados y con la seguridad de la información.

Ha sido diseñada con un espíritu duradero y práctico, de cara a contemplar nuevas normativas que puedan surgir de forma posterior a su entrada en vigor.

Es de aplicación toda la legislación y normativa vigente en relación con la protección de datos personales, propiedad intelectual y uso de herramientas telemáticas, y utiliza como referencia los siguientes estándares:

- ✓ RGPD: Reglamento General de Protección de Datos 2016/679 de la Unión Europea.
- ✓ TISAX: Trusted Information Security Assessment Exchange
- ✓ ISO/IEC 27001: norma que se centra en los requisitos para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI).
- ✓ ISO/IEC 27002: norma que se centra en los controles al implementar un SGSI, incorporando controles de acceso a datos, control criptográfico de datos confidenciales y administración de claves.
- ✓ Estándares requeridos por los grupos de interés, con especial respuesta a los de los clientes.

3. Principios básicos de la seguridad

- ✓ Aceptar como activos estratégicos la información y los sistemas que la procesan y almacenan, manifestando su determinación en alcanzar los niveles de seguridad necesarios para garantizar su protección, y así mejorar la calidad de los servicios ofrecidos a los empleados o clientes.
- ✓ Garantizar la confidencialidad de la información manejada para la adecuada prestación de los servicios, adaptando las medidas de seguridad al nivel de confidencialidad exigido sobre la información manejada.
- ✓ Garantizar la disponibilidad de la información y de los sistemas que la procesan y almacenan, estableciendo las medidas de prevención, detección y recuperación de carácter organizativo, físico y lógico necesarias.
- ✓ Gestionar los riesgos a los que se ve sometida la información mediante la identificación de posibles amenazas y la adopción de medidas de seguridad apropiadas para tratarlas.
- ✓ Disponer de un entorno de seguridad que garantice el cumplimiento de los requisitos legales aplicables a la información y a los sistemas.

4. Medidas para garantizar la seguridad de la información

Con el fin de garantizar la existencia de un marco global de seguridad de la información que proteja, en la medida de lo posible, frente a dichas amenazas, el Comité de Seguridad de CIE Automotive procederá a adoptar una serie de medidas para prevenir, detectar, reaccionar y recuperarse ante posibles incidentes que afecten a la información.

La seguridad de la información es entendida como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

Se llevarán a cabo diferentes iniciativas que respalden los esfuerzos ya realizados, de cara a proporcionar una visión general sobre la seguridad de la información a todas las partes interesadas, definir los controles adecuados para proteger los activos y cumplir con los requisitos marcados por la legislación vigente.

En este sentido, se deberá poner en marcha los mecanismos adecuados para prevenir, detectar, reaccionar y recuperarse a los posibles incidentes que puedan afectar a la seguridad de la información. Entre dichos mecanismos se encuentran, entre otros, las siguientes medidas:

4.1. Prevención

Se tratará de prevenir y evitar la existencia de incidentes que puedan afectar a la seguridad de la información y a los servicios prestados. Para ello, se implantarán las medidas y controles de seguridad necesarios, que serán definidos a través de un proceso formal de análisis y gestión de riesgos.

Dichas medidas y controles, así como las responsabilidades en materia de seguridad de la información serán definidos y documentados de manera clara y formal tanto en la Política como en la Normativa de Seguridad de la Información.

Asimismo, y para garantizar el cumplimiento de la Política de Seguridad de la Información, a través de cada uno de sus departamentos, deberá:

- Participar activamente en el ciclo de vida de desarrollo de los sistemas, especialmente en la autorización de los mismos antes de entrar en operación.
- Realizar evaluaciones periódicas del estado de seguridad de la información, solicitando la revisión por parte de terceros para disponer de una evaluación independiente.

4.2. Detección y respuesta

Las medidas de prevención no son siempre suficientes ante incidentes de seguridad, por lo que se monitorizará de manera continua el funcionamiento de los sistemas de información de cara a identificar anomalías en su operación.

Ante la detección de un incidente de seguridad de la información, se pondrán en marcha los mecanismos de verificación, análisis y comunicación del mismo.

4.3. Recuperación

Para aquellos casos en que los incidentes causen un impacto importante, se dispondrá de planes de continuidad de los sistemas, asegurando que se encuentran integrados con los planes generales de continuidad de negocio y actividades de recuperación.

5. Marco organizativo

La seguridad de los activos de la información es responsabilidad de todos los departamentos de la empresa, así como de todas y cada una de las personas que interaccionen con los mismos.

No obstante, el Consejo de Administración de la Sociedad tiene atribuida la coordinación, dentro de los límites legales, de las estrategias y directrices generales de gestión del Grupo, operando en interés de todas y cada una de las sociedades que lo integran, correspondiendo, por su parte, al presidente del Consejo de Administración y consejero delegado y a los altos directivos de la Sociedad la función de organización y coordinación del Grupo mediante la difusión, implementación y seguimiento de la estrategia y políticas generales establecidas por el Consejo de Administración.

Al amparo de lo anterior, el Consejo de Administración de la Sociedad, a través de su Comisión de Auditoría y Cumplimiento, velará por el seguimiento de los principios y buenas prácticas que se contienen en esta política corporativa por parte de las sociedades integradas en el Grupo.

La Comisión de Auditoría y Cumplimiento delegará a su vez en el Comité de Seguridad la supervisión y cumplimiento de esta política. Este comité tendrá las siguientes funciones para garantizar la seguridad de la información y de los activos relacionados con esta:

- ✓ Revisar, al menos de forma anual, esta política y aprobar la normativa que la desarrolla.
- ✓ Establecer los medios necesarios para que tanto la política como la normativa sean conocidas por todos los afectados.

El Comité de Seguridad estará compuesto por los representantes corporativos de los departamentos de Sistemas de Información, Ingeniería, Recursos Humanos y Compliance. Asimismo, este comité contará con miembros permanentes y miembros invitados en función de la situación y los condicionantes de seguridad de la información.

Este comité designará a un Responsable de Seguridad de la Información, quien tendrá delegadas las siguientes funciones:

- ✓ Establecer los requisitos de la información en materia de seguridad, siendo responsable sobre el uso que se haga de la información relacionada con su ámbito de actuación, así como de su protección.
- ✓ Designar a una o varias personas competentes para ejercer las funciones relacionadas con los requisitos de seguridad de la información.
- ✓ Adoptar las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios, verificando que las medidas de seguridad establecidas sean adecuadas para la protección de los mismos y manteniendo el nivel de seguridad de la información dentro de su ámbito de actuación.
- ✓ Promover la realización de revisiones periódicas que verifiquen el cumplimiento de las obligaciones en materia de seguridad de la información, así como de promover la formación y concienciación en la compañía.

6. Seguimiento y control

CIE Automotive adoptará los mecanismos de control necesarios para asegurar, dentro de una adecuada gestión empresarial, el cumplimiento de la normativa, de los principios y las buenas prácticas enunciadas en esta política. Igualmente, dedicará a tales fines los recursos humanos y materiales adecuados y suficientemente cualificados. Se aprobarán y revisarán periódicamente unas directrices para evaluar y gestionar el riesgo identificado, aplicables a todo el Grupo, que incluirán unos criterios objetivos para clasificar las operaciones en función de su riesgo, así como distintos procedimientos para su aprobación.