## Planes de respuesta y supervisión para los principales riesgos de CIE Automotive

### *Las personas y el futuro de la organización*

En los últimos años, la falta de un plan de sucesión para el personal clave y de equipo humano para el crecimiento (orgánico e inorgánico) de CIE Automotive, así como la falta de formación y cantera se han revelado como algunos de los riesgos clave para la compañía.

Para reducir y minimizar estos riesgos, el Departamento de RRHH corporativo, en colaboración con la Alta Dirección y en coordinación con las distintas áreas geográficas, ha puesto en marcha un proyecto que incluye las siguientes iniciativas:

- Planes de contratación anuales de recién titulados con seguimiento personalizado desde cada División de Negocio.
- Planes de seguimiento personalizado de los perfiles con alto potencial.
- Planes de formación generales y personalizados. Así en los últimos años se ha producido un incremento constante en el número de horas de formación, hasta alcanzar las 34,1 horas anuales por cada trabajador.
- Planes de sucesión para puestos clave. Se han identificado los puestos clave para la consecución de los objetivos estratégicos de CIE Automotive, y se ha procedido a identificar a las personas sucesoras o estrategias a seguir, para asegurar que la organización, en caso de no poder contar con ellas, no se verá afectada.
- Plan de Desarrollo Profesional (PDP) para directivos y mandos intermedios de cada una de las Divisiones de Negocio.

## Cumplimiento del Código de Conducta

Durante 2016 y 2017 la organización realizó la distribución y firma del Código de Conducta con alcance global, y durante el ejercicio 2018 ha aprovechado el despliegue global de las Jornadas RSC para insistir en el cumplimiento del mismo, recordando que CIE Automotive dispone de un Canal Ético que es responsabilidad de la Comisión de Responsabilidad Social Corporativa, bajo la gestión colegiada de la dirección corporativa de los departamentos de Recursos Humanos, Cumplimiento y Asesoría Jurídica, para que cualquier empleado del grupo pueda formular denuncias sobre cuestiones ligadas al incumplimiento de las pautas de conducta indicadas.

*(Ver información adicional en apartado 3.3 Relación con los grupos de interés, apartado Despliegue global de las Jornadas RSC)*

## Cambio en las tendencias del mercado

En el sector de automoción pueden producirse cambios disruptivos para los que CIE Automotive tiene que estar preparado. Hoy día la organización está trabajando para tener flexibilidad ante las nuevas tendencias y adaptarse así a las necesidades actuales o futuras de los clientes.

*(Ver información adicional en apartado 4.2 Plan Estratégico 2016-2020)*

## Ciberseguridad

La ciberseguridad, entendida como la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados, se ha convertido hoy en día en uno de los mayores riesgos a los que se enfrentan las empresas.

Es por ello que CIE Automotive ha comenzado en 2018 un proyecto para la protección de dichos activos con una metodología de reingeniería de procesos e ingeniería social, basada en los principales estándares de referencia internacional con objeto de gestionar la seguridad de la información en tiempo real, manteniendo la trazabilidad de todos los procesos de gestión de seguridad.

## LÍNEAS DE ACTUACIÓN EN MATERIA DE CIBERSEGURIDAD

| | |
|---|---|
| **SERVICIO SOC** *(Security Operations Center)* | • Validación y recomendaciones sobre las políticas de seguridad a implantar.<br>• Monitorización de los servicios 24x7.<br>• Detección temprana de alertas.<br>• Seguimiento de incidentes de seguridad.<br>• Soporte de Cumplimiento Normativo<br>• Realización de auditorías para verificación del estado de la seguridad.<br>• Control de actuaciones de usuarios que vayan en contra del manual de buenas prácticas. |
| **SERVICIO SIEM** (Security Information and Event Management) | • *Critical Events Detection*: Plataforma para la detección de eventos de alto riesgo en entornos corporativos: aquellos que consiguen evadir los sistemas de seguridad desplegados, como correos maliciosos que alcanzan los buzones de empleados y de VIPs, *malware* en USBs o dispositivos corporativos comprometidos.<br><br>• *Cyber Threat Intelligence*: agrega y analiza información de multitud de fuentes, proporciona inteligencia de contexto a la información que generan las infraestructuras IT, permite detectar eventos de alto riesgo en redes corporativas y puede integrarse con elementos de seguridad ya existentes para ejecutar acciones de mitigación en tiempo real. |
| SERVICIO *INCIDENT RESPONSE* | • Servicio de gestión de incidencias y activación ante crisis de una naturaleza relevante. |

CIE Automotive ha definido, además, una sistemática de evaluación y priorización de riesgos a nivel de centro productivo y con alcance global. Esta evaluación involucra a todo el equipo directivo de cada centro productivo y se realiza siguiendo el mapa de procesos, definiendo para cada uno de los mismos la tipología de riesgos que pueden afectarles y evaluándolos de forma binaria, en función de sus impactos y nivel de ocurrencia, estableciendo, en definitiva, una priorización de los mismos. Su minimización o eliminación, si esta fuese posible, se convertirá en un objetivo más a considerar dentro del plan de gestión de cada centro productivo.

Además, en las plantas ya realizan diferentes análisis de riesgos a través de herramientas como:

- AMFE (Análisis Modal de Fallos y Efectos) de productos y procesos productivos.
- Identificación y evaluación de impactos medioambientales.
- Evaluación de riesgos de seguridad y salud de las personas.
- Evaluación del cumplimiento legal.
- DAFO.