¿Cumple Identity-C con la normativa existente en materia de protección de datos?

En el desarrollo de la solución Identity-C, han sido analizadas y puestas en práctica tanto las normativas como las recomendaciones y dictámenes en materia de protección de datos relacionados con el tratamiento de datos biométricos, en particular:

- RGPD Reglamento 2016 679
- LOPD GDD 3/2018
- Dictamen 3/2012 Evolución de las tecnologías biométricas (GT29)
- La protección de datos en las relaciones laborales (AEPD)

Bases jurídicas para la implementación de Identity-C

Las bases jurídicas sobre las que se sustenta el tratamiento de datos realizado por el sistema de control de accesos y registro "Identity-C" son:

- **Cumplimiento de obligaciones legales** por parte del responsable (Estatuto de los trabajadores) en materia de registros de jornadas de los trabajadores. El artículo 20.3 del ET otorga el derecho al empleador para la implantación de medidas de control de las personas trabajadoras.

- **Interés Legítimo** por parte del empleador para implementar un mecanismo que verifique con precisión que sólo acceden a las obras personal autorizado e informado de los riesgos elevados que existen en los espacios interiores al perímetro de la obra.

Proceso de desarrollo de solución. Cooperación entre actores

Identity-C ha sido desarrollado gracias a la colaboración entre Cibinar y el Departamento de PRL de Acciona, por lo que los puntos de vista entre actores (Desarrollador / integrador y responsable del tratamiento / requisitos de solución) han sido puestos en común, creando una solución basada en el principio de desarrollo **desde el diseño y por defecto**.

Proporcionalidad del sistema

Siguiendo el RGPD y las recomendaciones de la AEPD, el sistema ha sido testeado con respecto al principio de proporcionalidad:

- **Idoneidad**: La naturaleza de alto riesgo que presenta una obra de construcción obliga al empleador a tomar medidas de control orientadas a que sólo accedan al espacio personal autorizado. Además, el carácter vivo de una obra (diferentes horarios de entrada/salida, proveedores, subcontratas y trabajadores propios), requiere un exhaustivo control a lo largo de toda la jornada de trabajo, incluidos nuevos equipos de trabajo desconocidos por el responsable de obra, por lo que el sistema debe almacenar la fotografía como elemento de verificación humana por parte del responsable. Las obligaciones de portar, por parte de cualquier trabajador, los EPIs necesarios para el desarrollo de los diferentes tajos han de ser revisados por razones de seguridad y salud en obra, por lo que almacenar las imágenes forenses del cumplimiento de EPIs en el acceso responde a un interés legítimo del empleador en caso de accidente. Por último, es común en ambiente de obras las pérdidas y olvidos por parte de los trabajadores de elementos accesorios menos invasivos como tarjetas RFID, dispositivos móviles, o tarjetas identificativas.

- **Necesidad**: La existencia de otros métodos en el control de accesos menos invasivos (Tarjetas RFID, códigos de acceso, etc.) son insuficientes para realizar un control de accesos preciso que permita al empleador realizar el control de jornada de los trabajadores, por lo que, hasta ahora, era necesario que personal de seguridad y salud realizara registros manuales a lo largo del día. La naturaleza de los tajos a realizar, unido a las distancias entre éstos y los puntos de acceso regulados provocan retrasos en los accesos de trabajadores y proveedores, y suponen unos costes no despreciables para realizar dichos controles. Además, la Visión Artificial es la única tecnología existente que permite corroborar de manera automatizada que los trabajadores acceden a sus puestos de trabajo portando los EPIs necesarios, por lo que su implementación resulta una necesidad.

En este contexto, Identity-C resuelve cada una de los objetivos propuestos minimizando los riesgos de exposición del tratamiento de datos.

Por tanto, y dada la idiosincrasia del sector de aplicación, la automatización de los procesos de control de accesos resulta de una eficiencia muy elevada con respecto a sistemas de control tradicionales.

- **Proporcionalidad**: La medida no vulnera la vida privada de los trabajadores, ya que se siguen los principios básicos en materia de tratamiento de datos personales, y solo persigue una identificación del personal que accede por su propia seguridad. Así mismo, existe sistema alternativo de acceso en el que la intervención humana resuelve cualquier inconveniente (posibles falsos rechazos del sistema de reconocimiento facial). Además, se ha aplicado en el desarrollo el principio de protección de datos desde el diseño y por defecto para mitigar los posibles riesgos existentes.

Características del sistema con respecto a las recomendaciones RGPD-AEPD

En el desarrollo del sistema han sido tenidas en cuenta las recomendaciones existentes en materia de protección de datos:

- **Minimización de datos**: Identity-C utiliza una imagen del trabajador para crear una plantilla o vector digital, siendo el único dato personal necesario para el proceso de identificación. Los datos de contacto asociados a dicho trabajador son proporcionados por la empresa responsable del tratamiento.
- **Limitación de finalidad**: La finalidad de la tecnología es realizar un control de accesos y EPIs, así como automatizar los registros de jornada de los trabajadores. Los datos obtenidos no serán tratados ulteriormente y el sistema no está destinado al procesado de otros datos como raza, edad, o emociones del usuario.

- **Periodo de conservación**: Identity-C incorpora un proceso de supresión automatizada de dichos datos en el momento en que el tratamiento deja de tener base jurídica (finalización de obra o fin de autorización de acceso al trabajador).
- **Tratamiento de datos en bases de datos reducidas**: Las bases de datos con la que Identity-C trabaja son reducidas (personal autorizado a acceso en obra), por lo que el riesgo de uso ilícito es bajo.
- **Tasa de rechazo**: El sistema Identity-C incorpora un mecanismo de intervención humana con contacto directo al responsable de obra para resolver los posibles errores del sistema (FRR) y ofrecer al trabajador un método alternativo en el acceso a su puesto de trabajo.
- **Sistema Anti usurpación**: El sistema de identificación desestima los procesos no continuos en el tiempo, y consta de fases en las que se validan los elementos EPIs necesarios, por lo que no es posible realizar usurpaciones al sistema mediante fotografía.
- **Cifrado de datos**: El sistema incorpora un cifrado de las plantillas biométricas de los usuarios como medida Técnica en caso de uso ilegítimo de los datos obtenidos.
- **Integridad y confidencialidad**: Cibinar, como empresa especializada en Ciberseguridad, aplica diferentes técnicas de codificación, denegación de acceso, y anti extracción al sistema Identity, por lo que los riesgos de uso ilícito de los datos han sido analizados y mitigados sobremanera. Además, Cibinar cuenta con la ISO 27001, (Seguridad de la información) que garantiza la confidencialidad de los datos tratados en los procesos en los que interviene.
- **Transferencia de datos entre empresas**: La naturaleza de una obra implica diferentes actores en la gestión de datos (Sistema CAE, Subcontratas, Empresa encargada de la obra), entre los cuales ya existen procedimientos legales para la transferencia de datos personales de trabajadores. Cibinar, como empresa de mantenimiento del sistema, tiene acceso a dichos datos, y responde a sus obligaciones legales mediante la formalización de los contratos de tratamiento en función de la naturaleza del servicio, adaptándose a los procesos del cliente.

¿Debe realizarse un Estudio de Impacto de protección de datos?

En este sentido, la AEPD pone de manifiesto las diferencias entre los sistemas que se detallan a continuación:

- **Identificación**: La identificación de un sujeto consiste en predecir si éste forma parte de un grupo en un proceso de comparación uno-a-varios (1:n). La ventaja de este sistema radica en que no es necesario portar elementos adicionales (dispositivos, tarjetas RFID, códigos de acceso…) por parte de los trabajadores y, por tanto, es el método más adecuado para las obras de construcción. Estos datos se consideran de categoría especial y para el uso de esta tecnología es necesario realizar previamente un Estudio de Impacto.

- **Verificación**: La verificación de un sujeto consiste en la comprobación de que es quien dice ser. Para ello, se realiza un proceso de comparación uno-a-uno (1:1), comparando su vector biométrico con la plantilla almacenada del sujeto. El inconveniente de este procedimiento radica en que el trabajador debe portar un elemento adicional que indique la plantilla con la que deben comparase su vector. Este dato no es considerado dato de categoría especial, por lo que no es necesario desarrollar un Estudio de Impacto.

Dada la naturaleza de una obra, Identity – C está diseñado para realizar un proceso de identificación para responder a las dificultades que conlleva portar elementos adicionales, por lo que es necesario realizar un Estudio de Impacto.

Recomendaciones al cliente

De manera adicional a las medidas técnicas y organizativas analizadas e implementadas en el sistema, Cibinar recomienda:

- **Informar de forma transparente** a los trabajadores del nuevo sistema de control y presencia, sus derechos, los datos tratados (puntos biométricos), su finalidad (control de accesos y seguridad EPIs) y el fin del tratamiento (Fin de autorización de acceso a la obra), momento en el cual todo dato almacenado será suprimido de manera automatizada.
- **Trasladar a los representantes de los trabajadores** la nueva medida y su finalidad: Aumentar la seguridad de los trabajadores en obra (Control de EPI´s y denegación de acceso a personal no autorizado potencialmente peligroso) y aumentar la eficiencia administrativa de la compañía (Registro de horarios automatizado).