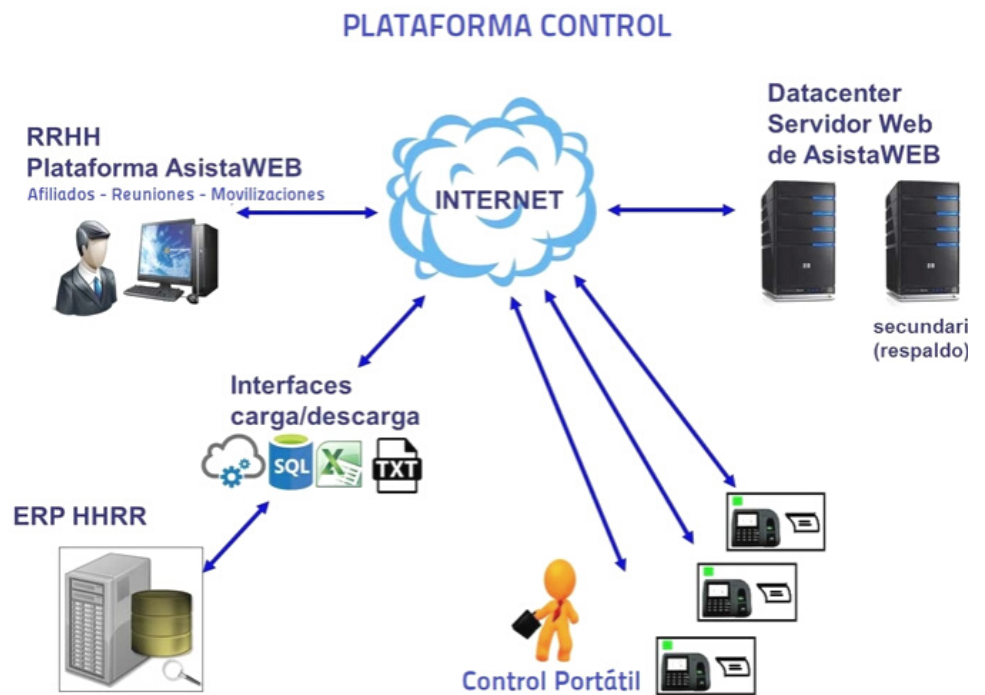


CONTROL BIOMÉTRICO

SISTEMA DE CONTROL CON HUELLA PARA INGRESO Y SALIDA DE EMPLEADOS CON INFORMES PARA LA DIVISIÓN DE TALENTO HUMANO

Software y Hardware de última generación

El control de acceso biométrico es un sistema de identificación basado en las cualidades biológicas del usuario. Dentro de este sistema, podemos diferenciar entre diferentes tipos de reconocimiento. Puede ser por huella dactilar, facial, ocular o vascular



LA MODERNIZACIÓN PERMITE MÁS SERIEDAD Y EFICIENCIA EN LA EJECUCIÓN DE TAREAS

Un sistema de control biométrico permite registrar las horas de entrada y salida de los trabajadores usando la huella digital de las personas para identificar cada empleado y evitar el fraude. El uso de estos datos (huella dactilar, reconocimiento facial y lectura de iris) no deja de expandirse adaptándose a las necesidades más cotidianas de la vida privada como desbloquear smartphones y ordenadores personales. Mientras llega el «imperio de la voz», que será la emisión personal más utilizada dentro de muy poco, lo irreplicable de los rasgos físicos individuales garantiza un alto nivel de seguridad como herramienta de identificación y autenticación ya que estas características físicas convertidas en parámetros estadísticos logran una exactitud por vía matemática que se está imponiendo en el mercado del control.

Los defensores del empleo de la huella dactilar resaltan que es un método de identificación considerado fiable desde que el policía francés Alphonse Bertillon la introdujera en el siglo XIX como elemento identificativo.



ALTERNATIVA DE VALOR

Los sistemas de control de accesos biométricos reconocen a sus usuarios y admiten o restringen la entrada a un recinto mediante su conexión a una cerradura electrónica. No solo permiten conocer quién ha accedido a una instalación y a qué hora, sino que también posibilitan llevar un registro de esa actividad. Su mayor ventaja es soslayar incidencias de otros medios identificativos que pueden perderse o ser cedidos a otras personas pervirtiendo la función de control, como las tarjetas o las llaves.

Una vez realizada su instalación y la inversión inicial, este tipo de control de accesos tiene un coste de mantenimiento inferior al de otros sistemas y son muy seguros al manejar parámetros «casi» imposibles de simular. Este «casi» es una salvedad razonable, porque todo sistema que se apoye en software y/o codificaciones ha de contar con el «elemento hacker». Así lo hacen las universidades y empresas tecnológicas volcadas en el perfeccionamiento continuo de la seguridad de los sistemas. audi

”

Cada centro de trabajo conoce sus requerimientos mejor que nadie, y se aconseja en mayor medida el reconocimiento facial O DIGITAL

