Executive Brief

Cloud, cumplimiento normativo y la transformación de RR.HH. para apoyar su estrategia de gestión del capital humano (HCM)

Patrocinado por: ADP

Duncan Brown Alexandros Stratis

Noviembre 2016

RESUMEN EJECUTIVO

Los líderes de RR.HH. se enfrentan al desafío de los enfoques tradicionales relativos al tratamiento de los datos de los empleados. Este puede variar de manera significativa entre la central y las filiales, por una combinación de factores como el uso de diferentes aplicaciones de software, proveedores de servicios de externalización y centros de datos distribuidos. Asimismo, la adopción generalizada de la nube (cloud) supone una presión aún mayor desde el punto de vista de las normas de seguridad.

Para hacer frente a estos desafíos y a la necesidad de ser más estratégicos de cara al negocio, los responsables de recursos humanos están liderando proyectos de transformación y realizando inversiones en tecnología de RR.HH. Un factor determinante para obtener el retorno esperado de estas iniciativas es trabajar con un proveedor de tecnología de RR.HH. que pueda garantizar una integración consistente entre la política de protección de datos y el cumplimiento normativo dentro de sus servicios y ofertas de software.

La gestión del capital humano (HCM) está sufriendo una rápida transformación que está remodelando la gestión de la fuerza de trabajo.

La gestión del capital humano (HCM) está sufriendo una rápida transformación que está remodelando la gestión de la fuerza de trabajo. Esto viene impulsado por la evaluación del rendimiento en base a proyectos, colaboración y resultados, el compromiso general con los empleados, y la manera en que éstos pueden planificar sus carreras y su futuro. El departamento de RR.HH., que ha sido tradicionalmente el responsable de los registros de los empleados, el administrador de la formación y el ejecutor de las transacciones de recursos humanos, se está ahora transformando en un socio estratégico para el crecimiento de la organización.

Un elemento clave de esta transformación en la gestión del capital humano implica que tanto las soluciones propietarias como los procesos manuales estén rápidamente dando lugar a soluciones comerciales y servicios en la nube pública (public cloud). La adopción de soluciones cloud probablemente proporcione un mayor alcance funcional de usuario para los clientes, aportando además la eficiencia y flexibilidad de las arquitecturas cloud.

Pero las preocupaciones por la seguridad persisten. Confiar información sensible a terceros es siempre un paso importante, pero colocar los datos de los empleados en la nube, un lugar desconocido y protegido apenas por unas vagas promesas de seguridad, resulta insuficiente para la mayoría de los responsables de RR.HH. ¿Cómo puede el empresario asegurarse de que los datos de los empleados están a salvo?

Este problema es mucho más serio si lo analizamos tanto en términos de obligaciones como de consecuencias. El reglamento general de protección de datos (General Data Protection Regulation, GDPR), que entrará en vigor el 25 de mayo de 2018, incrementa los requisitos de seguridad y

de aquellas otras actividades ligadas al tratamiento de datos personales susceptibles de conllevar riesgo. Es importante destacar que el GDPR es un reglamento, no una directiva, lo que significa que aplica de igual manera a los 28 estados miembros sin necesidad de transformarse en una ley a nivel nacional.

A la luz del GDPR, las empresas están encontrando dificultades para entender y dar respuesta a los cambios regulatorios a medida que se van produciendo. Los costes y los riegos de no conformidad pueden ser significativos.

La nube, siempre y cuando esté correctamente implementada, puede mitigar los riesgos de no conformidad con el GDPR y con las leyes laborales locales. En opinión de IDC, numerosas compañías decidirán externalizar el tratamiento de los datos de su personal para reducir el riesgo y sus obligaciones de cumplimiento. Pero un proveedor de servicios de externalización de recursos humanos deberá tener un sólido plan de acción, mapas de flujo de datos, planes de conservación de datos, robustas plataformas de seguridad y programas de transferencia de datos, todo ello con el soporte de la Oficina de Protección de Datos (Data Protection Office, DPO).

La nube, siempre y cuando esté correctamente implementada, puede mitigar los riesgos de no conformidad con el GDPR y con las leyes laborales locales.

Este informe explica el impacto del GDPR y pone de relieve cómo las soluciones cloud pueden permitir - en lugar de impedir - el cumplimiento normativo, mejorando simultáneamente su estrategia HCM digital.

El GDPR representa el mayor cambio de una ley de protección de datos en tres décadas.

EL CAMBIANTE ENTORNO REGULATORIO DE LOS DATOS DE RR.HH.

El GDPR representa el mayor cambio de una ley de protección de datos en tres décadas. Por un lado, actualiza la ley anterior, previa a la emergencia de Facebook, LinkedIn y la nube, y por otro unifica la legislación de protección de datos a través de los 28 estados miembros.

La directiva de protección de datos existente se aprobó en 1995 y no es adecuada para la protección de los datos personales de los individuos en un mundo en que el almacenamiento e intercambio online de información de carácter personal es cosa habitual. Además, la directiva fue implementada por cada estado miembro conforme a sus costumbres y culturas de negocio, lo que dio lugar a una gran disparidad de regímenes de protección de datos a través de la Unión Europea. El GDPR representa por tanto un gran paso adelante en la homogeneización y modernización de la ley de protección de datos en Europa.

El GPDR otorga idénticos derechos a los datos de los empleados que a los de los clientes.

La definición de datos de carácter personal es muy amplia: incluye toda aquella información que puede o podría permitir la identificación directa o indirecta de un individuo. Esto incluye los identificadores obvios como nombre o número de identificación, pero también los datos de ubicación o dirección IP, así como la información biométrica o genética. Es importante destacar que entre los datos de carácter personal figuran tanto los de los empleados de una empresa como los de sus clientes.

Tal vez sea obvia la principal implicación del GDPR sobre los datos de RR.HH., pero merece la pena mencionarla. El GPDR otorga idénticos derechos a los datos de los empleados que a los de los clientes. Esto significa que se incrementan las obligaciones de la compañía con respecto a la protección de sus datos de RR.HH., que se refuerzan los derechos de acceso, rectificación y anulación de los datos por parte de los empleados, y que las consecuencias del no cumplimiento son graves, como veremos más adelante.

Sin embargo, los departamentos de RR.HH. no están solo limitados por el entorno relacionado con el GDPR y la privacidad de los datos. El número de reglamentos que han de cumplir, propios de

cada país, es un desafío en sí mismo. RR.HH. debe asegurar el cumplimiento en cinco áreas diferentes: beneficios y seguros, selección y contratación, seguridad y riesgos laborales, contabilidad de la nómina y gestión del ciclo de vida del empleado.

Las organizaciones piden cada vez más a sus departamentos de RR.HH. que sean proactivos y se involucren en toda clase de "riesgos relacionados con las personas" en cada una de las cinco áreas mencionadas. El riesgo es aún más complejo para las organizaciones que trabajan en diferentes jurisdicciones, con filiales o matrices en diferentes ubicaciones. Lo importante aquí es entender que el cumplimiento en el ámbito de RR.HH. se debe ver como una función general de gestión del riesgo que también potencia la agenda de recursos humanos.

Además, el cumplimiento ayuda a elevar el papel de RR.HH., pasando de ser un sistema de registros con una mínima función estratégica a ser un socio estratégico capaz de reducir los costes relacionados con los riesgos, además de incrementar la productividad y el compromiso de los empleados.

Los ejemplos de requisitos de cumplimiento para los departamentos de RR.HH. que requieren de constante monitorización y gestión de sus parámetros, pueden ir desde las contribuciones de nóminas e impuestos (el sistema PAYE en Reino Unido comparado con el "impuesto sobre la renta" en Francia, etc.), formación (incorporación, detección de fraude, etc.) y requisitos de desarrollo profesional (seguimiento de los Créditos de Desarrollo Profesional/CPD u otras métricas utilizadas por las asociaciones profesionales y comités para asegurar la pertenencia) hasta la auditoría en los procesos de contratación y rescisión.

CARACTERÍSTICAS FUNDAMENTALES DEL GDPR

Como se ha mencionado, la definición de datos de carácter personal en el GDPR es muy amplia. Desde la perspectiva de RR.HH., se protege cualquier información relativa a un empleado, e incluso se prohíbe recoger determinadas categorías de datos. Esto incluye a las llamadas "categorías especiales" de datos, a menudo denominadas también datos sensibles. Estas categorías de datos incluyen los datos genéticos, biométricos y de salud, así como la preferencia u orientación sexual. Sin embargo, una salvedad importante con respecto a esta prohibición reside en el tratamiento de la información para su uso en medicina preventiva o laboral, o para la evaluación de la capacidad de trabajo de un empleado (Artículo 9 del GDPR).

El GDPR también introduce una responsabilidad y una obligación conjuntas, en algunos casos, entre aquellos que controlan los datos (normalmente el empresario, en el contexto de los RR.HH.) y aquellos que realizan el tratamiento de esta información (terceros que tratan los datos en nombre del empresario). Este es un tema importante para cualquier empresario que externaliza o está pensando en externalizar el tratamiento de RR.HH.

En lo que respecta a los requisitos de seguridad, el GDPR es deliberadamente vago. De los 99 artículos del texto final del GDPR, solo uno (el artículo 32) se refiere específicamente a la provisión de la seguridad, y no ofrece demasiados detalles. Las principales instrucciones del reglamento indican que las organizaciones deberían tener en cuenta los últimos avances en tecnología, así como los costes, el riesgo y el contexto empresarial. Por tanto, las organizaciones tendrán que decidir lo que significa para ellas la "tecnología puntera"; no es una tarea sencilla. El artículo también recomienda encarecidamente (aunque no obliga) el cifrado y la seudoanonimización (equivalente a la tokenización en términos generales).

Sin embargo, es importante destacar que la seguridad constituye una parte fundamental de los principios relativos al tratamiento de los datos de carácter personal (Artículo 5). Concretamente, el GDPR exige que los datos se traten de manera que "se garantice la adecuada seguridad de los

datos de carácter personal". Por tanto, aunque el GDPR es impreciso con respecto a las medidas a tomar para garantizar la seguridad, es explícito en cuanto a la importancia de la misma.

Desde el punto de vista de HCM, el GDPR hace que los responsables de RR.HH. tengan que tomar una serie de decisiones tecnológicas clave. Aunque no sea un requisito, muchos responsables de RR.HH. llegan a la conclusión de que es deseable cifrar todos los datos de los empleados, tanto cuando están simplemente almacenados como cuando se están transmitiendo o están en copias de seguridad. El GDPR no obliga a mantener registros de los tratamientos de datos ni a disponer de soluciones para facilitar las auditorías, tanto a efectos forenses como de cumplimiento normativo.

GDPR: más que seguridad

Una idea errónea muy generalizada acerca del GDPR es que es fundamentalmente un reglamento sobre la seguridad de los datos. Si bien la seguridad de los datos, como se ha mencionado, es un aspecto importante del GDPR, es un error considerar que la seguridad es la tecnología fundamental en juego. Hay otros requisitos que implican una gran variedad de tecnologías más allá de la seguridad.

Por ejemplo, el requisito de portabilidad de datos (Artículo 20) crea el derecho de un individuo a solicitar sus datos personales al controlador, en formato digital si fuera posible, cuando su tratamiento se basa en la aceptación del individuo o en un contrato. El derecho de cancelación (a menudo conocido como el derecho al olvido, Artículo 17) permite a un individuo exigir al controlador el borrado de sus datos personales, bajo una serie de circunstancias concretas y con algunas excepciones. Y las reglas para el consentimiento — en particular la recogida del consentimiento parental sobre los datos de los menores (Artículo 8) — se restringen duramente.

Uno de los aspectos clave del GDPR, como demuestran los siete artículos que le dedica, es la transferencia de datos (Artículos 44 a 50). Las transferencias de datos implican el movimiento de información a un denominado país tercero. Un país tercero es aquel que no es miembro de la UE. El objeto es garantizar que los controladores protejan los datos de manera adecuada incluso fuera de su jurisdicción. La UE tiene dos mecanismos para contener esta amenaza: el control de las transferencias de datos más allá de la UE y una cláusula de extraterritorialidad que extiende el ámbito del GDPR a cualquier tipo de dato relacionado con una persona en la UE (independientemente de la ubicación de los datos; ver Artículo 3).

El GDPR es impreciso con respecto a las medidas a tomar para garantizar la seguridad; es explícito en cuanto a la importancia de la misma.

Las transferencias de datos son importantes en el contexto de los datos de RR.HH. cuando los empresarios utilizan servicios basados en la nube o proveedores de servicios de externalización de RR.HH. Conocer el lugar en que residen los datos físicamente, y en particular si se encuentran fuera de la UE, constituye un requisito legal para los empresarios. La exportación de datos fuera de la UE es perfectamente legal; sin embargo, se debe hacer teniendo en cuenta alguno de los diferentes mecanismos de supervisión reglamentaria. Estos incluyen:

- Transferencias sobre la base de la idoneidad: la UE mantiene una lista de países con leyes de protección de datos consideradas adecuadas (o equivalentes) al GDPR. Solo hay 12 países en esa lista y (detalle importante para muchos) los EE.UU. no están entre ellos.
- Normas Corporativas Vinculantes (BCR, por sus siglas en inglés): se trata de un compromiso por parte del responsable del tratamiento de los datos de implementar un programa de protección de datos con un alto nivel de protección de los mismos, de acuerdo con el GDPR, aprobado por las autoridades de protección de datos de la UE. No es una decisión fácil, y demuestra un compromiso vinculante y duradero con los principios de protección de la privacidad de la UE.

- Cláusulas del modelo estándar incluidas en el contrato.
- Consentimiento por parte de los afectados a la transferencia de sus datos fuera de la UE.
- Adhesión a un código de conducta aprobado o a un mecanismo de certificación. Ambas estructuras están promulgadas en el GDPR, pero aún están pendientes de implementación.

El otro mecanismo fundamental para las transferencias de datos legales se da cuando existe un acuerdo específico entre la UE y el país tercero. Este enfoque se utiliza normalmente cuando no ha sido concedida una decisión de idoneidad. El mejor ejemplo de esta situación es el Privacy Shield, un acuerdo bilateral entre EE.UU. y la UE que permite la transferencia de datos a los responsables de tratamiento adheridos al acuerdo. Sin embargo, el Privacy Shield probablemente se someta a los tribunales, como lo fue su predecesor, el Safe Harbor. IDC opina que las empresas con sede en EE.UU. que quieran demostrar su compromiso a largo plazo con los principios del GDPR deberían seguir la senda de las BCR.

Una oportuna ilustración del régimen de transferencia de datos es por supuesto el Brexit. El Brexit es en gran medida irrelevante en lo que se refiere a la protección de datos. Esto se debe a las reglas de transferencia de datos del GDPR: si cualquier empresa de Reino Unido desea comerciar con un socio de la UE, o tratar datos de carácter personal de la UE, tendrá que suscribir las reglas de transferencias de datos incluidas en el GDPR. Dado el volumen de negocio actual entre Reino Unido y la UE, es probable que el primero adopte una ley similar al GDPR cuando abandone la UE. De hecho el ICO (Information Comissioner's Office) ya lo ha indicado.

Multas por incumplimiento

Se han dedicado numerosos titulares a las multas administrativas "eficaces, proporcionadas y disuasorias" potencialmente impuestas por los organismos reguladores. En particular, se ha prestado especial atención a las multas máximas de hasta un 4% de la facturación global anual o de 20 millones de euros, la mayor de ambas cifras. Merece la pena destacar que ese nivel de multas solo es aplicable a infracciones relativas a los principios del GDPR (Artículo 5), derechos fundamentales de los interesados, tales como la aceptación y la cancelación, así como las violaciones en las transferencias de datos. Las violaciones de datos personales en sí, como resultado por ejemplo de vulnerabilidades en la seguridad, están sometidas a niveles menores de multa, hasta un 2% de la facturación global anual o 10 millones de euros. Los empresarios pueden preocuparse en mayor medida por la obligatoriedad de notificación de las infracciones. Los controladores de datos deben notificar a la autoridad supervisora correspondiente cualquier caso de violación de datos de carácter personal que resulte en un "riesgo para los derechos y libertades individuales" (Artículo 33). En estos casos, también deben comunicar el incidente a los propios individuos (Artículo 34). Esto podría conducir a una publicidad negativa, que podría posteriormente perjudicar a la marca y a la reputación.

El Brexit es en gran medida irrelevante en lo que se refiere a la protección de datos.

Finalmente, una autoridad supervisora ostenta el poder de ordenar la suspensión del tratamiento de datos (Artículo 58). Esto podría traducirse de hecho en una orden de cese de la actividad comercial o de la ejecución del proceso de nómina, si el tratamiento de datos en cuestión soportase un proceso clave de negocio.

Teniendo en cuenta estas sanciones, no sorprende que el GDPR esté acaparando la atención de los miembros de los comités ejecutivos de las empresas de la UE (y de fuera de la UE, por la extraterritorialidad). Sin embargo, es importante entender que las sanciones (como las multas) se impondrán probablemente en los casos en que se carezca de evidencias de un esfuerzo por cumplir con la normativa. El GDPR hace un fuerte énfasis en la demostración del cumplimiento normativo, incluyendo la creación y el mantenimiento de registros

del tratamiento de datos. La auditabilidad es crítica, y la capacidad de demostrar el cumplimiento (responsabilidad) es un principio básico del GDPR.

EL CASO DE LAS SOLUCIONES CLOUD: POR QUÉ AYUDAN, EN LUGAR DE LASTRAR, LAS OPERACIONES DE RR.HH.

Los servicios cloud constituyen en esencia una forma de externalización. Como para cualquier actividad de externalización, se debe proceder con la auditoría del proveedor. Los tratamientos de RR.HH. basados en la nube deben por tanto someterse al mismo nivel contractual de auditoría.

Sin embargo, la nube es diferente en términos de la multiplicidad de factores involucrados. Las empresas han de abordar la auditoría de manera práctica mediante diversas preguntas sobre el nivel de seguridad y los procesos de protección de datos existentes, y mediante el análisis de informes de auditoría, incluyendo los informes independientes de terceros, posiblemente facilitados por el proveedor de servicios cloud. Resulta crítico, por ejemplo, entender la seguridad física del centro de datos en que se alojan los datos de carácter personal. Un proveedor de confianza dispondrá al menos de una solución en materia de seguridad tan buena como la de la mayor empresa, y probablemente considerablemente superior a la de la organización de un empresario medio. Incluirá probablemente la certificación ISO 27001 y (cada vez más) 27018, centrada en los datos de carácter personal en las nubes públicas.

No existe por tanto ningún impedimento legal ni técnico para el almacenamiento de datos de recursos humanos en la nube. Algunas empresas pueden optar por una configuración con un centro de datos ubicado en la UE, con certificaciones probadas de seguridad física y seguridad lógica. Además, el acceso a los datos de la UE se debe producir únicamente desde el interior de la UE: el acceso desde el exterior constituiría una transferencia de datos (efectuado por datos en tránsito) y disminuiría la eficacia de los centros de datos de la UE.

No existe ningún impedimento legal ni técnico para el almacenamiento de datos de recursos humanos en la nube.

La mayoría de las soluciones cloud requerirán transferencias de datos en el exterior de la UE en menor o mayor medida. Los proveedores han desarrollado soluciones para proteger los datos de carácter personal que incluyen modelos de cláusulas contractuales. Pero las normas corporativas vinculantes (BCR) están emergiendo como la forma más sólida de garantía jurídica para abordar las transferencias de datos.

Numerosas compañías decidirán externalizar el tratamiento de los datos de personal para reducir su riesgo y sus obligaciones de cumplimiento normativo. Los empresarios no pueden eliminar el riesgo, pero la selección de un proveedor fiable es una acción adecuada.

LOS PROVEEDORES DE TECNOLOGÍA Y SU PAPEL EN LA TRANSFORMACIÓN Y EL CUMPLIMIENTO NORMATIVO DE RR.HH.

Las normas corporativas vinculantes están emergiendo como la forma más sólida de garantía jurídica para abordar las transferencias de datos.

Se dice a menudo que las empresas pueden externalizar el tratamiento, pero jamás la responsabilidad. En lo que se refiere al GDPR esto sigue siendo válido, pero la ampliación de la responsabilidad para incluir a los responsables del tratamiento implica que al menos parte de la responsabilidad del cumplimiento se pueda trasladar a un tercero, proveedor de tratamiento de datos.

Para que quede claro, el controlador sigue siendo responsable y debe ser capaz de demostrar el cumplimiento de los principios fundamentales del GDPR (Artículo 5). Pero el principal requisito para el responsable del tratamiento de los datos es que sea capaz de implementar las medidas, tanto a nivel técnico como a nivel organizativo, acordadas

con un controlador. También se enfrenta a las mismas sanciones por incumplimiento. Esto plantea la siguiente pregunta: ¿cómo puede saber un controlador que el responsable del tratamiento es capaz de cumplir este requisito?

Los códigos de conducta y las certificaciones se establecen por ley al amparo del GDPR, pero hasta la fecha ninguno de estos mecanismos existen en la práctica. De modo que los responsables del tratamiento de la información pueden convencer de sus credenciales a los empresarios por medios complementarios, tales como certificaciones ISO 27001 (gestión de la seguridad de la información), 27018 (protección de datos de carácter personal en public cloud) o 29100 (marco de trabajo sobre privacidad), informes de auditoría independientes y BCR de los responsables del tratamiento, demostrando el compromiso de adhesión a los principios del GDPR por parte de la organización. Las autoridades de protección de datos de la UE consideran las BCR como el patrón de oro de la protección de datos.

Con el reloj ya en cuenta atrás hacia el 25 de mayo de 2018, las organizaciones empresariales no pueden ignorar el GDPR ni los cambios sustanciales que conlleva.

El desafío para los proveedores de servicios de Outsourcing de RR.HH. (HRO, por sus siglas en inglés) radica en conseguir eficiencias a través de múltiples organizaciones mediante las operaciones a escala, mostrando conocimiento de las leyes laborales y las prácticas locales. Deben ser al mismo tiempo internacionales desde el punto de vista operativo pero locales en el proceso de implantación. En la opinión de IDC, un escaso número de proveedores de HRO serán capaces de ofrecer esta combinación de capacidades.

Un aspecto importante para el profesional de recursos humanos es el hecho de que el negocio actual ve, quiere y espera más del departamento de RR.HH. Los antiguos sistemas de RR.HH. eran sistemas de registro, con escaso valor estratégico añadido para la organización, y enfocados exclusivamente hacia la gestión de los aspectos más simples en torno al ciclo de vida del empleado.

Un aspecto importante para el profesional de recursos humanos es el hecho de que el negocio actual ve, quiere y espera más del departamento de RR.HH.

Conforme pase el tiempo, con el cambio en las capacidades, reglamentos y lo que es más importante, en el papel que se espera que adopte RR.HH., el profesional de recursos humanos espera convertirse en más estratégico y más valioso para la organización en su totalidad. Bajo esta perspectiva, no se debe subestimar el cumplimiento normativo; por el contrario, la gestión del cumplimiento desde la perspectiva de RR.HH. se convierte en un factor fundamental para limitar los riesgos en el negocio, y tiene el potencial de reducir los costes y proteger de los litigios, a pesar del aumento en la complejidad y el alcance del rol del departamento de RR.HH.

PRINCIPALES RECOMENDACIONES

No ignore el GDPR

Ahora que el reloj ya ha empezado la cuenta atrás hacia el 25 de mayo de 2018, es importante que las empresas no ignoren el GDPR ni los cambios sustanciales que conlleva. El ámbito técnico y jurídico del GDPR es amplio, y la mayoría de las organizaciones tendrán dificultades para implementarlo en su totalidad para la fecha de su entrada en vigor. Si las organizaciones no han comenzado aún a analizar el impacto del GDPR, deberían empezar inmediatamente.

El GPDR es una oportunidad

Es fácil percibir el GDPR y toda la serie de cambios que implica como un serio obstáculo para la negociación y como una distracción de las actividades normales del negocio. En realidad, según IDC, el GDPR representa una gran oportunidad para las empresas. Crea un entorno regulatorio claro y uniforme para las transferencias de datos que sustentan los servicios HRO basados en la

nube. Con las garantías adecuadas en relación con la seguridad aportada por un proveedor, las empresas pueden utilizar servicios de HRO basados en la nube como parte de su estrategia de HCM.

El cumplimiento es colaboración

En agosto de 2016 IDC completó su *Encuesta sobre Gestión del Capital Humano* en Europa occidental, con más de 250 respuestas de ejecutivos y responsables de RR.HH. En nuestra encuesta, los asuntos de la privacidad de los datos y de los cambios en la legislación (GDPR) se revelaron como una de las principales preocupaciones para uno de cada tres encuestados, mientras que solo un 23% se mostró “algo preocupado” o “no preocupado en absoluto”. La mayoría de los consultados (76%) todavía considera la privacidad de datos y el cumplimiento (con el GDPR y demás legislación) como un factor que influye en la decisión de compra de una solución HCM.

Es crucial para los proveedores dotar a RR.HH. de las herramientas y el conocimiento necesarios, junto con la garantía de que las soluciones de sus portfolios son conformes y seguras. De esta forma podrán ayudar a los departamentos de RR.HH. a alcanzar sus objetivos a largo plazo, en concreto en la transformación de su función administrativa posicionándose como un socio valioso para la dirección.

Sobre IDC

International Data Corporation (IDC) es el principal proveedor mundial de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología de consumo. IDC ayuda a los profesionales, ejecutivos de negocios y a la comunidad de inversores en la toma de decisiones sobre compra de tecnología y estrategia de negocio basadas en hechos. Más de 1.100 analistas de IDC ofrecen información mundial, regional y local sobre tecnología, oportunidades y tendencias de la industria en más de 110 países de todo el mundo. Durante 50 años, IDC ha venido suministrando información estratégica para ayudar a nuestros clientes a alcanzar sus objetivos claves de negocio. IDC es una filial de IDG, el medio de comunicación líder en tecnología, investigación y eventos a nivel mundial.

IDC Reino Unido

IDC Reino Unido
5th Floor, Ealing Cross
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Derecho de autor y restricciones