

## Información sobre seguridad de Unisys: España

Perspectiva del consumidor - 2015



### La opinión del consumidor español acerca de:

- La seguridad de datos personales, clasificada por sectores
- El incremento de vigilancia para mantener la seguridad nacional

## Table of Contents

Resumen ejecutivo	3
La postura de Unisys	4
Conclusiones detalladas: 1) Riesgo de violación de datos	5
Diferencias demográficas esenciales por sector	6
Conclusiones detalladas: 2) Vigilancia de seguridad nacional	7
Diferencias demográficas esenciales	7
Perspectiva de Unisys sobre la seguridad	8
Metodología de la encuesta	9
Acerca de Lieberman Research Group	10
Acerca de Unisys	11

## Resumen ejecutivo

Unisys desempeña un papel fundamental en la lucha por combatir los riesgos a los que se exponen los servicios y productos tecnológicos que proporcionan a sus clientes en España. El compromiso de Unisys por la seguridad pública y financiera constituye el motivo de nuestro estudio en estas áreas.

La encuesta de información sobre seguridad de Unisys representa una radiografía del punto de vista nacional acerca de la seguridad en determinadas esferas de interés, la cual proporciona un indicativo estadístico de las preocupaciones del consumidor que permite a las entidades adoptar decisiones sobre seguridad mejor fundamentadas. El estudio lo elabora la compañía líder en estudios de mercado Lieberman Research Group.

Para la encuesta de 2015, se preguntó a los consumidores en España por sus percepciones acerca de:

- La seguridad de datos personales, clasificada por sectores
- El incremento de vigilancia para mantener la seguridad nacional

La encuesta preguntaba a los consumidores acerca del riesgo de que a lo largo del próximo año personas no autorizadas accediesen a sus datos personales –en posesión de organizaciones tales como líneas aéreas o empresas de transporte, entidades bancarias y financieras, organismos administrativos, servicios de atención sanitaria, comercios, compañías de telecomunicaciones y de servicios–.

La amenaza percibida frente a la seguridad de datos personales es mayor en el caso de las empresas de telecomunicaciones, con un 66% de los encuestados que prevé una violación de datos en los próximos 12 meses. Las líneas aéreas y compañías de transporte se percibieron como las menos expuestas a riesgo siendo solo un 23 por ciento de los encuestados el que considera que los datos del consumidor se comprometen de algún modo.

Los encuestados en España estimaron la seguridad nacional como de elevada importancia con el 100 por cien de los mismos a favor de un incremento en la vigilancia. Además, el 65 por ciento de los encuestados apoya la divulgación de transacciones bancarias y de tarjeta de crédito a la administración.

Estas conclusiones deben valer como recordatorio a empresas e instituciones en España para que revisen e implanten medidas de seguridad avanzadas, con el fin de proteger a los consumidores de amenazas tanto cibernéticas como físicas. Una mentalidad volcada en la seguridad es vital para que una organización pueda eficazmente mitigar un entorno de riesgo. El planteamiento de Unisys respecto a la seguridad va más allá de bits y bytes, ya que admite que las soluciones más efectivas serán aquellas generadas mediante la colaboración de intereses. Véase también [www.unisys.com/securityinsights](http://www.unisys.com/securityinsights)

Para más información acerca de lo que ofrece la seguridad de Unisys visite: [www.unisys.com/security](http://www.unisys.com/security)

## La postura de Unisys

### **La opinión española no confía ni en las compañías de telecomunicaciones ni en el gobierno en lo que respecta a la protección de datos personales**

Los resultados del estudio de Información sobre seguridad de Unisys 2015 demuestran que el consumidor español no confía ni en las compañías de telecomunicaciones ni en el gobierno español en lo que respecta a la protección de datos personales, con un 66 y 56 por ciento de los encuestados que considera que en estos respectivos sectores se producirán violaciones de datos durante los 12 próximos meses. En el otro extremo de la balanza, la menor amenaza de violación de datos que se percibe se corresponde con las líneas aéreas y los comercios (23 y 27 por ciento respectivamente).

Los resultados concluyen que los consumidores muestran relativamente pocas expectativas de que las organizaciones dispongan de datos personales sobre ellos y que desconfían de los controles de seguridad. Las organizaciones deberían aspirar a salvaguardar los datos de los consumidores mediante la implantación de soluciones que no solo mejoren la seguridad empresarial, sino que además inspiren confianza al consumidor.

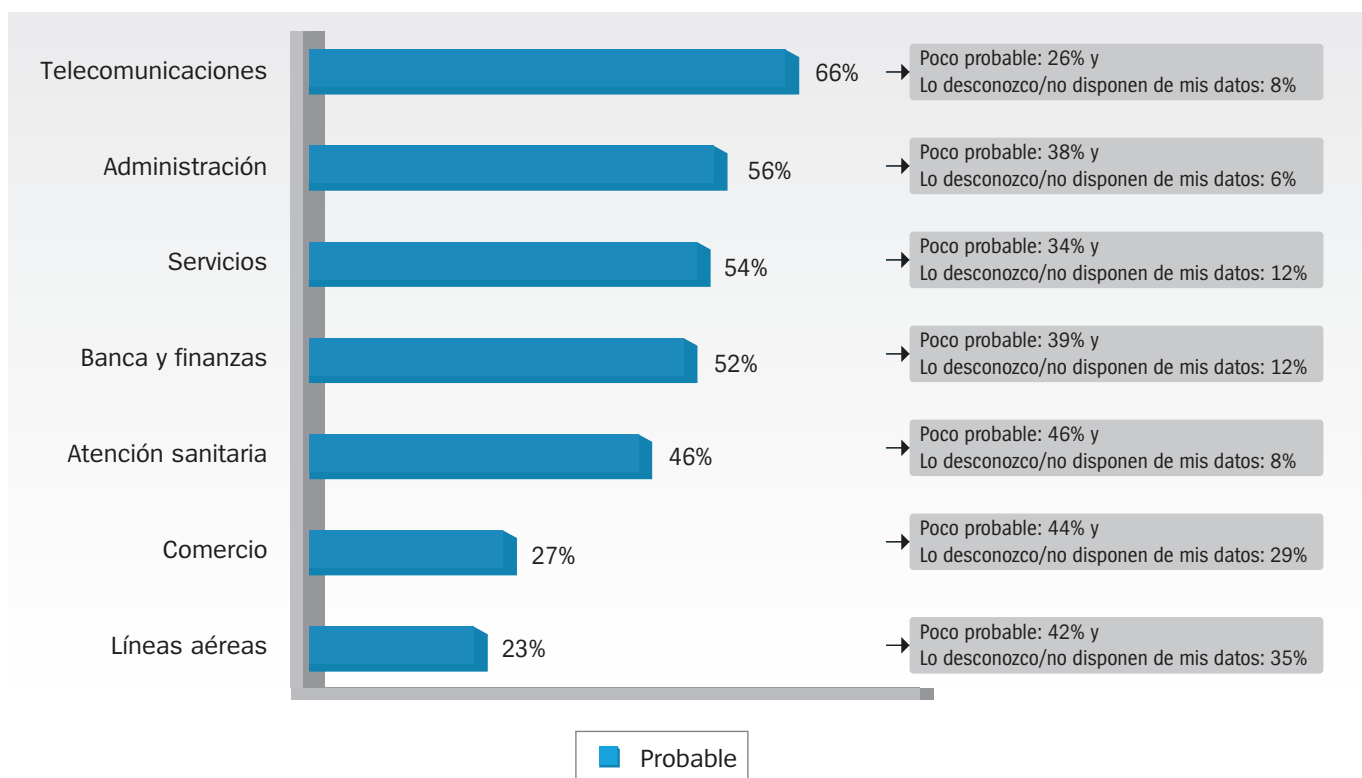
### **El consumidor español está a favor del aumento de vigilancia para mantener la seguridad nacional**

Como parte del estudio de información sobre seguridad de Unisys, también se preguntó a los consumidores acerca de sus opiniones sobre el incremento de vigilancia para el mantenimiento de la seguridad nacional. El estudio reveló que el 100 por cien de los consumidores están a favor de incrementar la vigilancia, con casi dos tercios (el 65 por ciento) siendo partidarios de la divulgación de transacciones bancarias y de tarjetas de crédito de las autoridades.

En un mundo en el que las amenazas de terrorismo, crimen organizado y ataques cibernéticos se perfilan como los asuntos de seguridad más relevantes, los resultados de la encuesta deben servir como recordatorio para que las entidades hagan todo lo que de ellas dependa para salvaguardar la seguridad del consumidor.

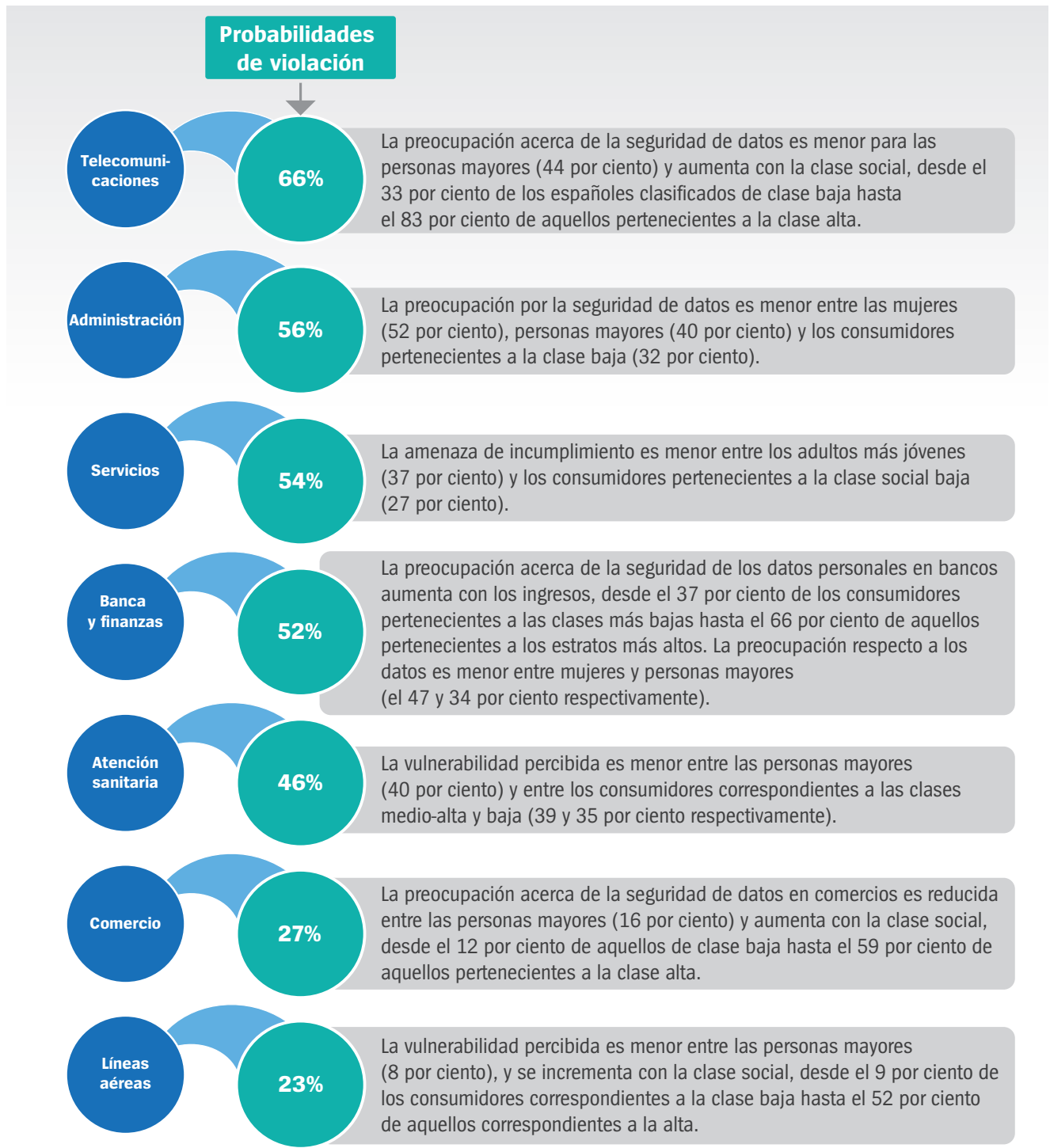
**Conclusiones detalladas: 1) Con respecto a cada uno de los siguientes tipos de organizaciones que recopilan datos personales suyos, ¿qué probabilidades considera que existen de que dentro de los próximos 12 meses una Persona no autorizada acceda, ya sea accidental o deliberadamente, a sus datos personales?**

La vulnerabilidad percibida de las compañías de telecomunicaciones y de los organismos públicos destaca en la opinión de los adultos españoles, con una mayoría de encuestados que estima que durante los próximos 12 meses se producirán violaciones de datos (66 y 56 por ciento). La aprensión por el acceso no autorizado también se muestra elevada en el caso de las empresas de servicios, bancos y en los servicios de atención sanitaria (54-46 por ciento).



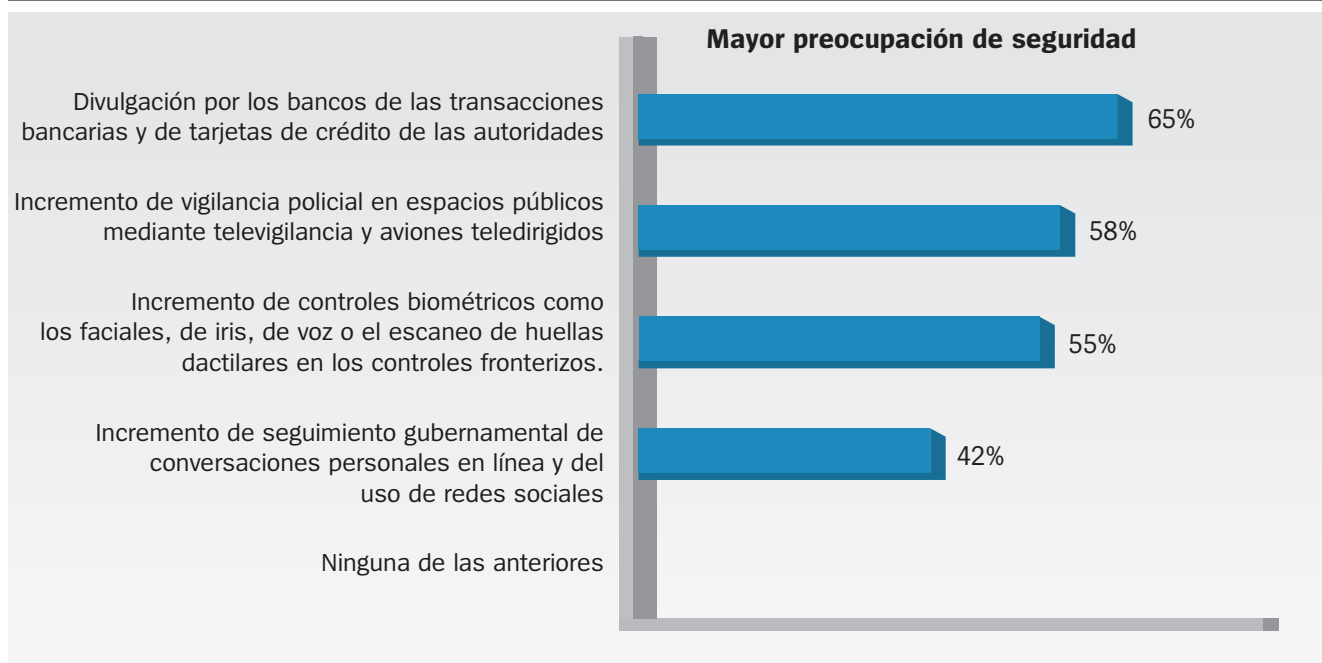
## Diferencias demográficas esenciales por sector

Las respuestas de los consumidores se analizaron en función de segmentos demográficos, edad y clase social. Las categorías de edad son 18-34, 35-49, 50-64 y mayores de 65 y las clases sociales se clasifican entre alta, medio-alta, media, medio-baja y baja.t



## Conclusiones detalladas: 2) ¿En qué áreas considera que deba incrementarse la vigilancia con el fin de defender la seguridad nacional?

Los españoles son partidarios del incremento de vigilancia, con casi dos tercios (65 por ciento) favorables a la divulgación de las transacciones bancarias y de tarjeta de crédito de las autoridades.



El 100 por cien de los españoles es partidario de incrementar al menos uno de estos tipos de vigilancia.  
Base = 98

### Diferencias demográficas esenciales

- Los bancos deberían divulgar las transacciones
- Mayor vigilancia de espacios públicos
- Más comprobaciones en los controles fronterizos
- Seguimiento de los publicaciones en línea y en redes sociales

Los consumidores pertenecientes a la clase más alta son más proclives a defender estas divulgaciones (el 82 por ciento).

El interés de los consumidores por el incremento de vigilancia aumenta con la edad, desde el 42 por ciento de los adultos jóvenes hasta el 71 por ciento de las personas mayores, y es menor para los españoles cuyo estatus se clasifica de medio-alto (50 por ciento).

Los consumidores cuyo estatus se clasifica de medio son más favorables a las comprobaciones de controles fronterizos (el 60 por ciento).

Los consumidores pertenecientes a la clase social más alta son más partidarios del seguimiento gubernamental de las publicaciones en línea y en redes sociales (58 por ciento).

## Perspectiva de Unisys sobre la seguridad

La encuesta revela que a los consumidores evidentemente les preocupa que las organizaciones dispongan de sus datos personales. La confianza de los consumidores se mostró reducida en general en el caso de las compañías de telecomunicaciones, las administraciones públicas y los bancos, ya que este tipo de organizaciones no ha conseguido adoptar medidas para recuperar la confianza perdida. Con una cada vez mayor hiper-conectividad de consumidores a través de varias plataformas digitales, los mecanismos tradicionales de protección de datos personales frente a ataques avanzados se revelan insuficientes. Para que las organizaciones puedan recuperar la confianza de cara a un entorno de seguridad tan incierto deberían adoptar:

- **Un planteamiento convergente de seguridad física y lógica** – Dado que las medidas lógicas y físicas están convergiendo, las principales empresas de todo el mundo deberían buscar modos de resolver los retos más críticos en el punto de convergencia. Tales medidas ayudan a integrar sensores, consolidar datos, proporcionar mando y control central o disperso, utilizar la información de identidad y permitir el análisis a tiempo real y fuera de línea. La seguridad convergente proporciona un seguimiento eficiente de la puerta al escritorio y a los datos.
- **Biométrica para una autenticación avanzada** – Una sólida estrategia de seguridad incorpora métodos de autenticación multifactor para garantizar la seguridad. La autenticación puede facilitarse mediante diversas técnicas biométricas como el reconocimiento facial, comparación de ADN, huellas dactilares, reconocimiento de voz la estructura venosa de las manos.

Al igual que las organizaciones, los dispositivos móviles también hacen uso de técnicas de autenticación avanzadas para evitar intrusiones y el robo de datos. Las organizaciones tienen la oportunidad de crecer a la par con las preferencias del consumidor y garantizar al mismo tiempo los estándares más elevados de protección.

- **Aislamiento y compartimentalización** – La protección de información confidencial frente al acceso no autorizado representa el objetivo fundamental para cualquier estrategia de seguridad. Normalmente esto implica las dos actividades cruciales de identificar el alcance de la protección de datos, y de aislar a las personas, procesos y tecnologías que interactúan con información confidencial. El aislamiento de datos se consigue mediante el empleo de controles de acceso y de encriptación para garantizar únicamente el acceso a la información confidencial a sistemas y usuarios autorizados. Además, la compartimentalización de grupos de usuario hace que se minimice la amenaza.
- **Una estrategia de seguridad integral** – El mantenimiento de capacidades de seguimiento, vigilancia y comunicación de seguridad avanzada dentro de un marco holístico de seguridad cibernética ayuda a proteger datos y redes frente a amenazas internas y externas. Una estrategia de seguridad integral abarcaría funcionalidades predictivas, preventivas, detectoras y retrospectivas.

Para más información acerca de lo que ofrece la seguridad de Unisys visite:

[www.unisys.com/security](http://www.unisys.com/security)



## Metodología de la encuesta

El estudio de información sobre seguridad de Unisys en España está basado en entrevistas personales realizadas entre

el 24 de abril y el 4 de mayo de 2015. La encuesta se realizó como sigue:

- se efectuaron 981 entrevistas íntegras entre adultos representativos a nivel nacional, de 18 años en adelante.
- La encuesta se realizó en español.
- Los datos obtenidos de esta encuesta se han ponderado para garantizar la proyección de los datos al español adulto. Los porcentajes se basan en las 981 muestras íntegras. Las diferencias de subgrupo solo se indican si estas son estadísticamente significativas con un grado de confianza del 95 por ciento.

## Acerca de Lieberman Research Group

Lieberman Research Group es una de las principales y más reconocidas entidades a nivel nacional que realizan estudios de mercado para los mercados empresariales y de consumo. Fundada en 1966, hoy en día es una empresa de servicios de investigación valorada en 30 millones de dólares. Los centros para realizar entrevistas en Manhattan y Brooklyn tienen capacidad para realizar entrevistas en más de 20 idiomas.

Lieberman Research es el único miembro estadounidense de The Global Research Alliance –un consorcio internacional de empresas de estudios de mercado independientes presente en más de 20 países que proporciona acceso a centros para realizar entrevistas a nivel internacional así como conocimientos e información de índole local determinantes para elaborar estudios internacionales óptimos.

Mediante sus estudios en EE.UU. y en el resto del mundo, Lieberman Research presta servicios de investigación y análisis de información a sus clientes con respecto a una amplia gama de asuntos, entre los que se incluye la satisfacción del cliente y del empleado, la fidelidad, el marketing multicultural y étnico, el desarrollo de nuevos productos, la política pública, la publicidad, las relaciones públicas y muchos otros.

Lieberman Research Group es miembro de las Council of American Survey Research Organizations (CASRO). Como una de las más de 150 compañías miembro de CASRO a nivel nacional, nos acogemos al código de normas de encuestas de CASRO.

Este código, cuyo propósito es el de fomentar los mayores estándares de conducta ética en la práctica de encuestas, protege a nuestros clientes y ayuda a garantizar un entorno en el que el público, nuestra fuente de información en la mayoría de las encuestas, respete y colabore con el proceso de estudio de opinión.

Aunque los no miembros pudieran también acogerse a estándares igualmente elevados que los de los miembros CASRO, la membresía en CASRO es un indicador de que nuestra compañía se toma muy en serio su obligación de desempeñar su actividad con arreglo a los estándares éticos más altos.



[www.casro.org](http://www.casro.org)

## Acerca de Unisys

Unisys es una compañía mundial de tecnología de la información que soluciona los retos empresariales y de TI más apremiantes de las organizaciones. Con más de 20.000 empleados prestando servicio a clientes de todo el mundo, ofrecemos, entre otros, servicios de infraestructura y en la nube, servicios de aplicación, servicios de externalización de proceso empresarial, y tecnología de servidor de primer nivel.

Prestamos servicio a 10 de los 15 principales bancos del mundo, 15 de las 25 principales líneas aéreas mundiales y a más de 200 líneas aéreas en todo el mundo. Se gestionan 10 millones de incidencias de usuarios en 26 idiomas diferentes cada año y los sistemas de Unisys procesan anualmente 130 millones de operaciones de servicios humanos y de salud. Nuestros procesos cumplen íntegramente con la ITIL v3 y cuentan con las certificaciones Global ISO 20000, 27001 y 9001. Unisys ostenta más de 1.500 patentes estadounidenses y no estadounidenses.

Clientes públicos y privados de todo el mundo confían en los servicios de seguridad de Unisys para prestar seguridad avanzada para hacer frente a amenazas avanzadas. Dado que las amenazas de seguridad lógica y física convergen, las empresas más importantes del mundo requieren un socio que ofrezca nuevos modos de resolver los retos más críticos en el punto en el que estas convergen. Nuestra galardonada, y con el tiempo reconocida cartera de servicios profesionales, productos y servicios gestionados ofrece seguridad crítica de alcance, que ayuda a los clientes a mitigar riesgos reduciendo complejidad y costes y operando conforme a los requisitos de conformidad regulatoria.

---

Para más información visite [www.unisys.com](http://www.unisys.com)

© 2015 Unisys Corporation. Todos los derechos reservados.

Unisys y otros productos y servicios de Unisys aquí mencionados, así como sus respectivos logos, son marcas registradas de Unisys Corporation. La propiedad del resto de marcas registradas aquí mencionadas corresponde a sus respectivos titulares.