

For the Complete Technology & Database Professional

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas?

Informe sobre la seguridad de los datos de IOUG 2008

Joe McKendrick, Analista de investigación, septiembre de 2008

Auspiciado por ORACLE
Producido por UNISPHERE

División de Information Today, Inc.

ÍNDICE

RESUMEN EJECUTIVO 3

ESTADO DE LA SEGURIDAD DE LOS DATOS EMPRESARIALES 5
FIGURA 1: Quién administra la seguridad de las bases de datos 5
FIGURA 2: Función de los encuestados en la seguridad de los datos 5
FIGURA 3: Violaciones o incidentes con los datos en el transcurso del año pasado 6
FIGURA 4: Probabilidad de una violación o incidente con los datos durante los próximos 12 meses 6
FIGURA 5: Cambio en el gasto en seguridad de IT durante el año pasado 7
FIGURA 6: Dónde radica la seguridad de las bases de datos en términos de las prioridades de la seguridad de IT 7
FIGURA 7: Seguridad de las bases de datos como una prioridad "Alta" para la seguridad de IT: por tamaño de la compañía 8
FIGURA 8: ¿Están todas las bases de datos de su compañía configuradas de forma segura? 8

DATOS RIESGOSOS Y VULNERABILIDADES 9
FIGURA 9: Los mayores riesgos, amenazas o vulnerabilidades para los datos empresariales 9
FIGURA 10: Áreas más vulnerables a violaciones o incidentes con los datos 10

SUPERUSUARIOS 11
FIGURA 11: ¿Se puede evitar que los superusuarios utilicen sin autorización datos delicados? 11
FIGURA 12: ¿Pueden los usuarios burlar aplicaciones y acceder directamente a datos de aplicaciones usando herramientas ad hoc? 11
FIGURA 13: ¿Se puede supervisar a los superusuarios para que no utilicen datos no autorizados? 12
FIGURA 14: ¿Están protegidos los datos de auditoría de bases de datos contra la utilización no autorizada de datos por parte de los superusuarios? 12

DATOS FUERA DE LAS INSTALACIONES 13
FIGURE 15: ¿Se subcontratan las funciones de administración de bases de datos? 13
FIGURA 16: ¿Se subcontratan o contratan servicios en el extranjero para las funciones de desarrollo o de prueba de bases de datos? 13
FIGURA 16: ¿Se envían fuera del sitio backups o exportaciones de bases de datos sin encriptar? 14

PROBLEMAS DE ENCRIPTACIÓN DE DATOS 15
FIGURA 18: Porcentaje de compañías que encriptan información de identificación personal en discos 15
FIGURA 19: Porcentaje de compañías que encriptan información de identificación personal en discos: por tamaño de la compañía 15
FIGURA 20: ¿Los datos de las aplicaciones se encriptan en la red cuando entran o salen de las bases de datos? 16
FIGURA 21: ¿Se encriptan todos los backups y exportaciones de bases de datos que se realizan en línea y fuera de línea? 16

PRUEBAS DE DATOS DELICADOS 17
FIGURA 22: Tipos de datos usados dentro de entornos que no son de producción 17
FIGURA 23: Porcentaje de compañías que envían datos de producción no encriptados con información delicada 18

SUPERVISIÓN Y AUDITORÍA 19
FIGURA 24: ¿Está supervisando actualmente todas las bases de datos de producción en busca de problemas de seguridad o cambios en la configuración? 19
FIGURA 25: Si supervisa regularmente las bases de datos de producción, ¿con qué frecuencia lo hace? 19
FIGURA 26: Actividades supervisadas regularmente 20
FIGURA 27: Porcentaje de encuestados preocupados por las auditorías de cumplimiento de los datos 20

CONCLUSIÓN 21

ASPECTOS DEMOGRÁFICOS 22
FIGURA 28: Número de bases de datos en las compañías de los encuestados 22
FIGURA 29: Principales funciones laborales de los encuestados 22
FIGURA 30: Compañías de los encuestados por número de empleados 23
FIGURA 31: Principales industrias de los encuestados 23

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

RESUMEN EJECUTIVO

El alcance de algunas de las mayores violaciones de datos en el mundo es legendario y ha ocupado titulares de la prensa internacionalmente: desde 94 millones de registros expuestos a través de un incidente de hackeo en TJX Companies Inc. en enero de 2007 hasta más de seis millones en Ameritrade en septiembre del mismo año.

No hay duda de que estos incidentes son costosos para las compañías. Junto con las pérdidas financieras directas, hay un costo incalculable para las organizaciones en términos de mala publicidad, pérdida de la confianza entre los clientes y exposición a posibles procesos judiciales.

Sin embargo, son los incidentes que no se ven y no se informan los que en realidad representan los mayores costos para las empresas. Por ejemplo, un administrador de base de datos contrariado puede tener acceso no detectado a datos de nómina de la compañía. El administrador no tiene que ser un empleado directo, puede trabajar para una compañía asociada que procesa regularmente datos delicados como números de tarjeta de crédito o de la seguridad social de sus clientes. No hay certeza de que la empresa asociada aplique prácticas seguras, como encriptación o desidentificación de datos delicados.

¿Cuán efectiva es la seguridad de las bases de datos en general? ¿Cómo perciben los gerentes y profesionales los problemas relacionados con la seguridad de las bases de datos? ¿Sienten que se está haciendo lo suficiente en cuanto a protección contra violaciones o incidentes internos con los datos? De acuerdo con los resultados de una nueva encuesta entre miembros del Independent Oracle Users Group (IOUG), no se está haciendo lo suficiente para abordar estos riesgos y vulnerabilidades en temas de seguridad de datos.

En julio y agosto de 2008, Unisphere Research realizó un estudio para IOUG con el fin de abordar estas y otras preguntas. La encuesta se realizó en cooperación con Oracle Corp. y fue anunciada a la lista de miembros de IOUG mediante una notificación por correo electrónico que dirigía a los participantes a un instrumento de encuesta basado en Web. En el plazo de la encuesta, se recopiló un total de 316 respuestas.

Con la encuesta se descubrió que mientras las organizaciones seguían estando preocupadas de la seguridad de IT en general y la mayoría apoyaba el concepto de seguridad de datos, pocas han abordado las vulnerabilidades clave que se derivan de la exposición de los datos a fuentes internas. La mayoría reconoce que las fuentes internas representan el mayor riesgo y la mayor vulnerabilidad, pero sólo una minoría ha abordado la seguridad para supervisar a los "superusuarios" como administradores con grandes privilegios de acceso, ya sea en línea o fuera de línea.

Esto se debe en parte a la complejidad de tener varios sitios de bases de datos. Muchos encuestados representan a sitios con grandes volúmenes de bases de datos. El 40% de los encuestados administra más de 100 bases de datos y el 20% administra más de 500 bases de datos.

De los 316 encuestados, el 57% indicó que eran administradores de bases de datos; el 9% se identificó como gerentes de IT; el 7%, como desarrolladores y, el 27% restante manifestó que desempeñaba una variedad de funciones, entre ellas consultor, arquitecto y gerente de proyectos.

Los encuestados provienen de una clasificación bastante homogénea de tamaños de compañías. Alrededor de un tercio, un 31%, provenía de organizaciones grandes con más de 10.000 empleados y, más de un tercio, un 35%, representaba a empleadores con un número de empleados que iba de 1.000 a 10.000. Además, el 30% representaba a firmas de tamaño más pequeño o mediano con 1.000 personas o menos. Por industria, el 15% provenía del sector de servicios y consultoría de IT y el 11% representaba a organizaciones gubernamentales. El 10% trabajaba en organizaciones educacionales y, otro 10% provenía de organizaciones de servicios financieros. (Para obtener información sobre los aspectos demográficos de esta encuesta, consulte desde la Figura 28 a la 31 al final de este informe).

Esta encuesta analizó un número de áreas de vulnerabilidad de datos, que incluyen la capacidad de supervisar las actividades de los superusuarios, el envío de datos fuera de las instalaciones, la encriptación de datos y el uso de datos delicados en entornos "que no son de producción", como en pruebas o preproducción. Finalmente, la encuesta examinó las prácticas de supervisión y auditoría en torno a los datos.

La encuesta descubrió que los encuestados están preocupados del potencial de los "superusuarios" (administradores, socios u otros empleados con privilegios de acceso) para comprometer maliciosa o accidentalmente los datos empresariales. Sin embargo, importantes segmentos de encuestados reconocieron que sus compañías no han implementado muchas de las medidas adecuadas que abordan la problemática de lo que sucede con los datos una vez que son sacados de los sistemas de producción y enviados fuera de las instalaciones para su administración o almacenamiento.

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para consultar resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

Entre los descubrimientos clave se incluyen:

Uno de cada cinco encuestados espera que se produzca una violación o incidente con los datos durante el próximo año. Solamente uno de cada cuatro sostuvo que todas las bases de datos están protegidas contra ataques.

Las organizaciones creen que los mayores riesgos se derivan del acceso interno, ya sea de usuarios no autorizados o de "superusuarios" como administradores con privilegios de acceso.

La mayoría de las organizaciones no ha implementado mecanismos para evitar que los administradores de bases de datos y otros usuarios de bases de datos con privilegios lean o alteren información delicada en aplicaciones financieras, de recursos humanos o en otras aplicaciones de negocios. La mayoría no puede ni siquiera detectar tales violaciones o incidentes.

Enviar datos a partes externas es ahora una práctica común.

Uno de cada cuatro sitios incluidos en esta encuesta no encripta los datos dentro de sus bases de datos y cerca de uno de cada cinco ni siquiera está seguro de si se realiza esta encriptación.

Dos de cada cinco organizaciones emplean datos de producción reales dentro de entornos que no son de producción, con lo cual exponen esta información en entornos sin seguridad.

Existe una creciente conciencia con respecto a los riesgos potenciales. La mayoría de las organizaciones supervisa sus bases de datos en busca de cambios que puedan ser indicadores de actividad maliciosa.

Para muchas compañías, lograr una estrategia que asegure varias capas de seguridad ha significado asignar la menor prioridad a la seguridad de los datos. Sin embargo, muchas están comenzando a reconocer la importancia de la seguridad de los datos. Como mencionó uno de los encuestados: "Nuestra compañía se ha concentrado en la seguridad de redes y servidores, como el acceso a nuestra red o servidores expuestos. La tendencia era no concentrarnos en sistemas o servidores internos, lo que incluía a muchas de nuestras bases de datos. Ahora que hemos logrado cumplir las normas y nuestro plan de recuperación ante desastres es sólido, nuestro encargado de seguridad pretende concentrarse en los problemas que no se han tenido en cuenta en el pasado, como la seguridad de las bases de datos".

En las siguientes páginas encontrará un resumen del alcance de las vulnerabilidades y riesgos que enfrentan las compañías con la seguridad de los entornos de datos.

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para consultar resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

ESTADO DE LA SEGURIDAD DE LOS DATOS EMPRESARIALES

Uno de cada cinco encuestados espera que se produzca una violación o incidente con los datos durante el próximo año. Solamente uno de cada cuatro sostuvo que todas las bases de datos están protegidas contra ataques.

Los encuestados representan a gerentes y profesionales de la información que están encargados directamente de la seguridad de los datos de sus organizaciones. En la mayoría de los casos, los encuestados indicaron que los gerentes y profesionales de bases de datos de sus compañías son directamente responsables de la seguridad de las bases de datos y, una mayoría de los encuestados de este estudio, un 93%, tiene la función de proporcionar seguridad a sus entornos de datos. (Consulte las Figuras 1 y 2).

FIGURE 1: Who Manages Database Security

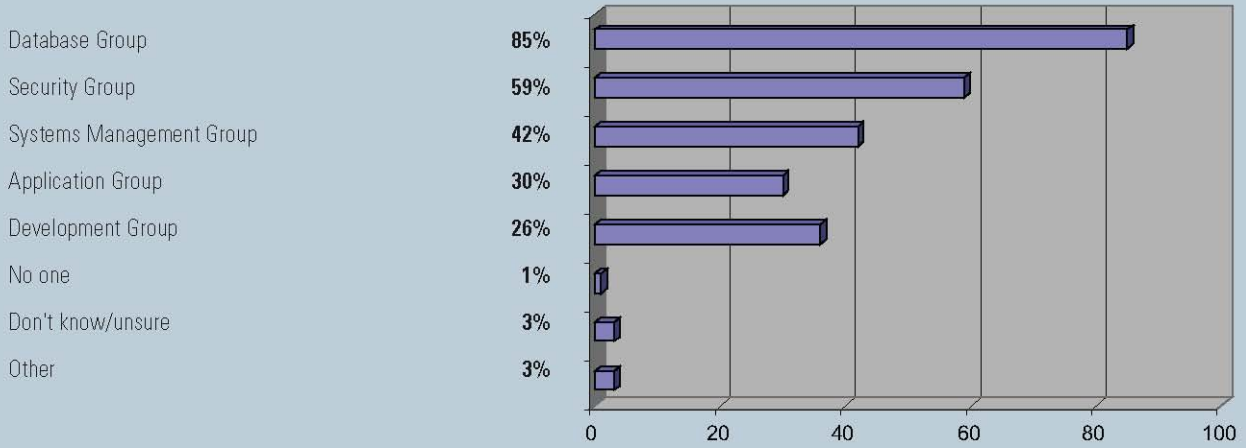
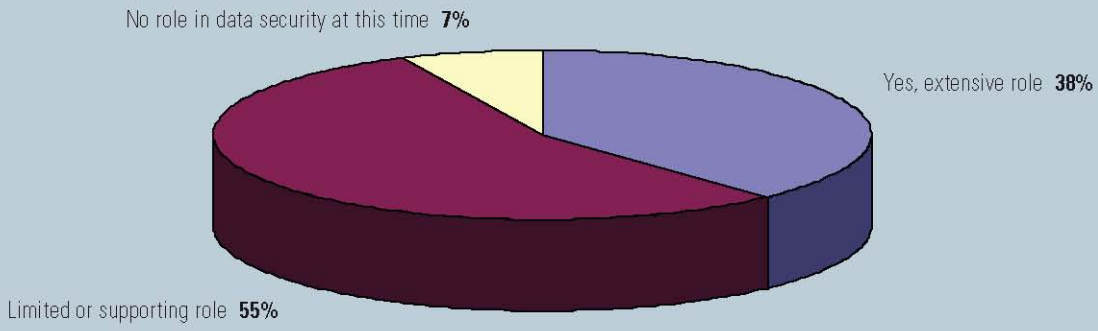


FIGURE 2: Respondents' Role in Data Security



Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para consultar resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

Alrededor del 6% de los encuestados informó de que durante el año pasado los datos de su compañía habían sido violados, comprometidos o alterados. Sin embargo, el 20% teme que puedan sufrir una violación o incidente con los datos dentro de los próximos 12 meses. (Consulte las Figuras 3 y 4).

FIGURE 3: Data Breaches or Incidents over the Past Year

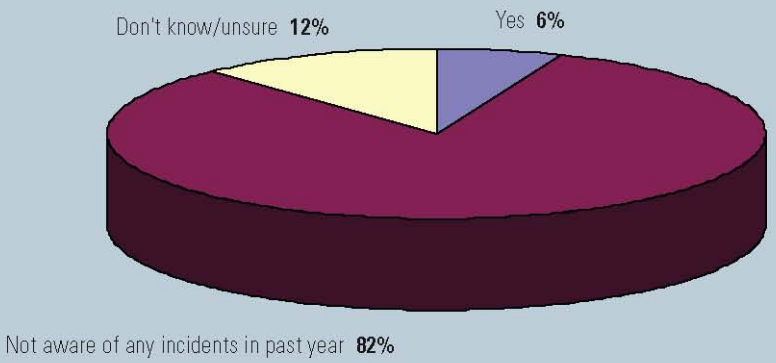
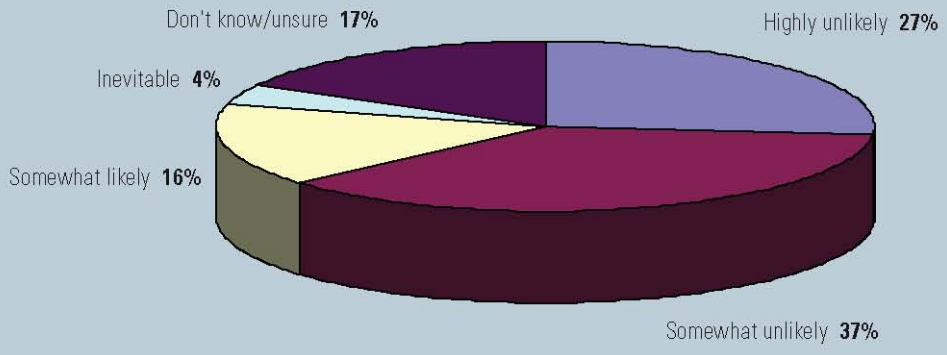


FIGURE 4: Likelihood of a Data Breach or Incident over the Next 12 Months

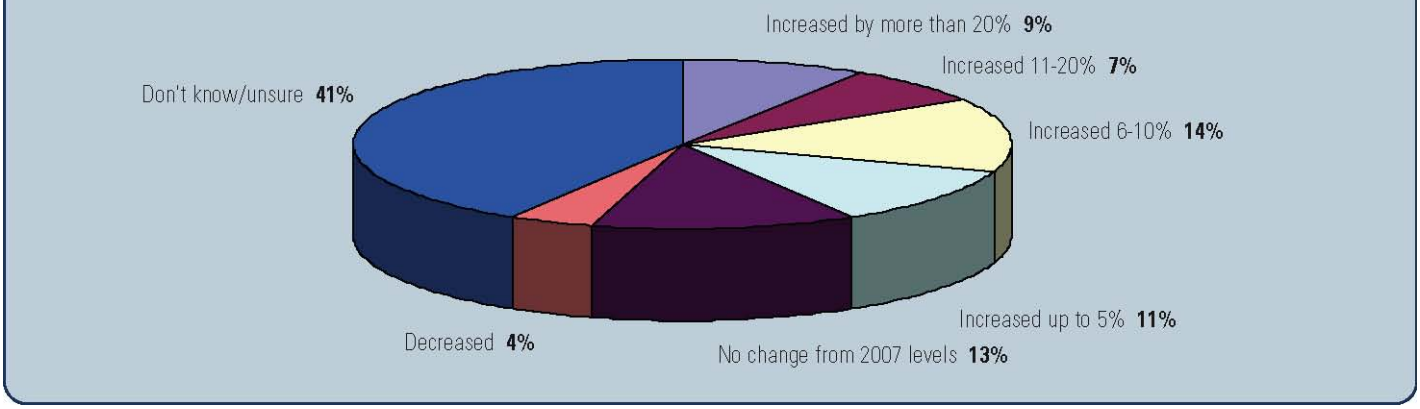


Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para consultar resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

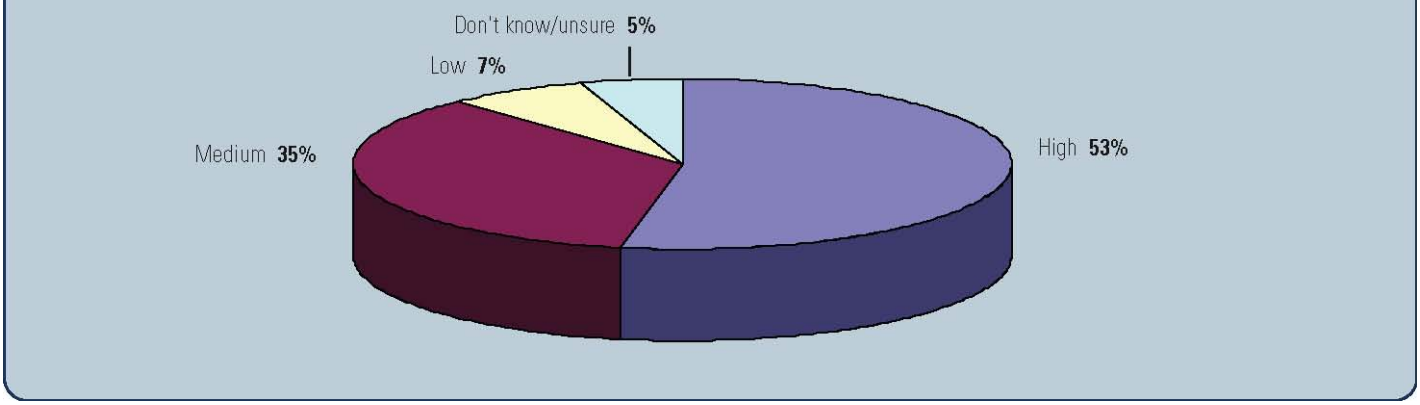
No hay duda de que para las compañías, la seguridad es una prioridad. Más de cuatro de cada 10 encuestados en este estudio (un 41%) informó de que el gasto relacionado con la seguridad había aumentado durante el año pasado y, sólo el 4% indicó que se había producido una disminución. Sin embargo, otro 41% simplemente no sabía cómo habían cambiado los niveles de gastos en seguridad de IT. (Consulte la Figura 5).

FIGURE 5: Change in IT Security Spending over the Past Year



La mayoría de los encuestados, un 53%, comentó que la seguridad de las bases de datos tiene una prioridad "alta" en la seguridad de IT dentro de sus compañías. Sin embargo, es revelador que el 12% calificara esta seguridad con un nivel de prioridad "bajo" o simplemente no conociera los niveles de seguridad de sus bases de datos. (Consulte la Figura 6). A mayor tamaño de la empresa, mayor es la probabilidad de que la seguridad de las bases de datos tenga una prioridad alta. (Consulte la Figura 7). La mayoría de los encuestados (un 58%) también coincide en que la infraestructura de su base de datos goza más o menos de la misma seguridad que otros activos de IT, como la infraestructura de red o los servidores de correo electrónico. En la mayoría de los casos, se aplican parches de seguridad a las bases de datos una vez cada cierto número de meses. Alrededor de una de cada cuatro compañías aplica parches de seguridad en cuanto están disponibles, pero el 47% comentó que esperaba hasta un año.

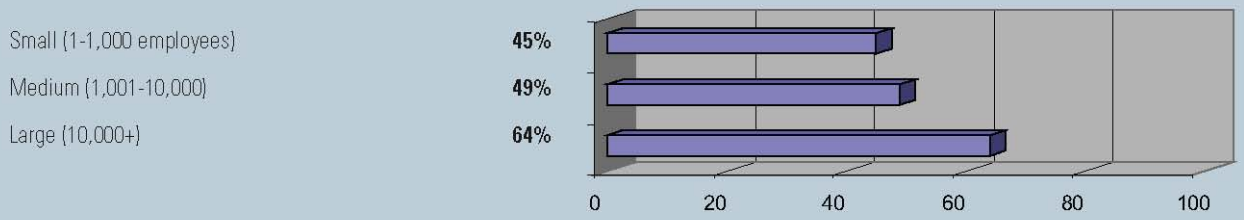
FIGURE 6: Where Database Security Falls in Terms of IT Security Priorities



Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para consultar resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

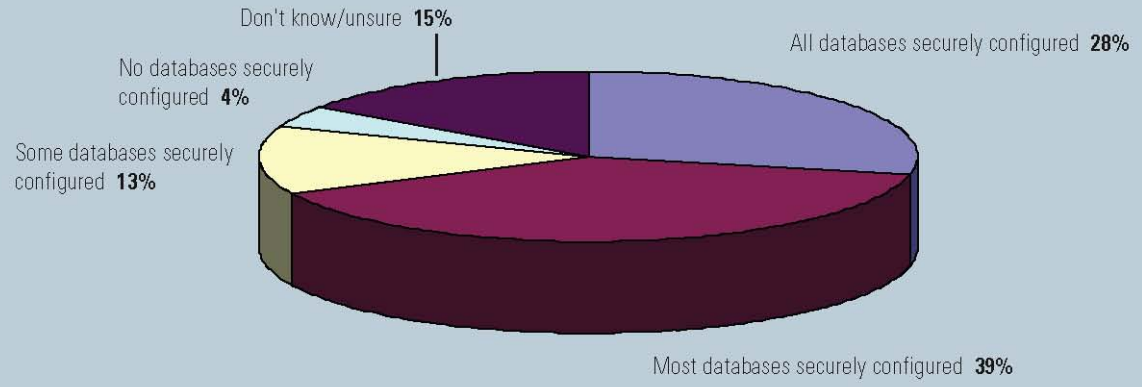
Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

FIGURE 7: Database Security as a "High" IT Security Priority - By Company Size



Existen pruebas de que la mayoría de las compañías tiene al menos algunas de sus bases de datos configuradas adecuadamente. Ocho de cada diez encuestados informó de que al menos algunas de sus bases de datos están configuradas de forma segura. Sin embargo, sólo el 28% podía afirmar que esta protección abarcaba todas sus bases de datos dentro de sus dominios. (Consulte la Figura 8).

FIGURE 8: Are all the databases in your enterprise securely configured?



Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para consultar resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

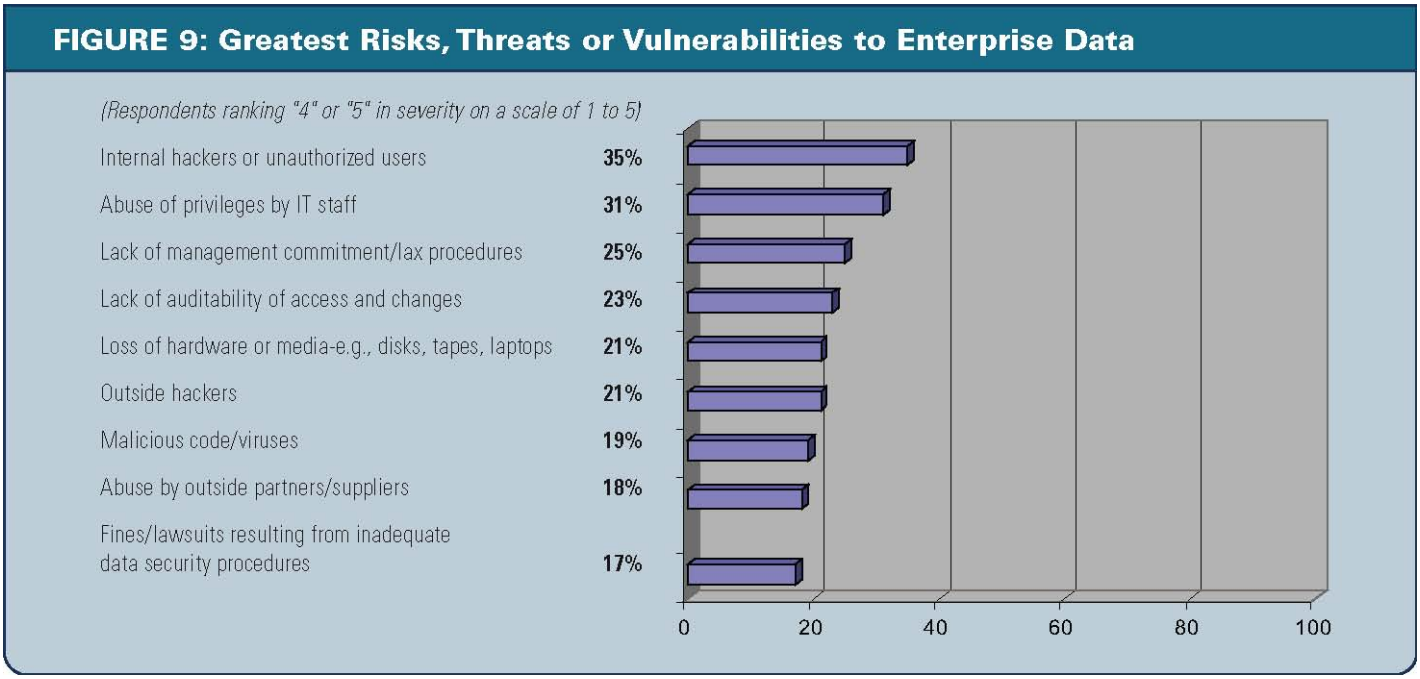
Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

DATOS RIESGOSOS Y VULNERABILIDADES

Las organizaciones creen que los mayores riesgos se derivan del acceso interno, ya sea de usuarios no autorizados o de "superusuarios" como administradores con privilegios de acceso.

Se solicitó a los encuestados que clasificaran el grado de vulnerabilidad a varios tipos de violaciones o incidentes con los datos en una escala de "1" a "5", donde 5 representaba la mayor amenaza a la vulnerabilidad. Los encuestados están más preocupados por las amenazas de hackers internos o usuarios no autorizados: más de un tercio, el 35%, calificó esta forma de vulnerabilidad con un "4" o un "5". A esta situación le sigue la preocupación por el abuso de privilegios del personal de IT, que fue citada como una vulnerabilidad importante por el 31% de los encuestados. Uno de cada cuatro encuestados citó la falta de compromiso de la gerencia y procedimientos poco estrictos, como las causas de exposición de sus datos a riesgos. (Consulte la Figura 9).

FIGURE 9: Greatest Risks, Threats or Vulnerabilities to Enterprise Data



Como se muestra en este informe, esta preocupación está bien fundada. Los datos son más vulnerables que nunca y muchas organizaciones informaron de que a veces los enviaban a socios externos o a personal subcontratado o que se extraían de las transacciones para utilizarlos en otras partes de las organizaciones. La mayoría de las organizaciones carece de salvaguardas o mecanismos de supervisión para proteger los datos contra violaciones o incidentes internos.

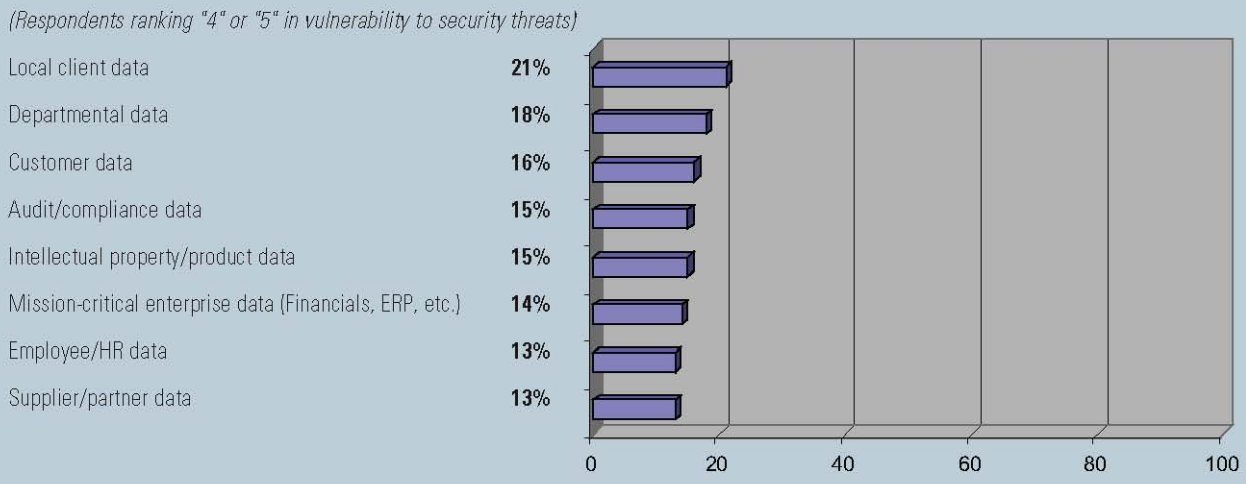
"Pese a que existen procedimientos para dar seguimiento y supervisar estas actividades, el mayor desafío proviene de la administración del personal que tiene acceso privilegiado", comentó un encuestado. Otro encuestado lamentó que en su compañía no se haya definido la más mínima seguridad de acceso para los empleados internos. Los empleados hacen todo a su manera y no siguen ninguna pauta estricta".

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

Dentro de los entornos altamente distribuidos de hoy, los datos fuera del control de la empresa se consideran como la mayor vulnerabilidad. Los encuestados de este estudio calificaron los datos almacenados en equipos cliente locales como el tipo de datos más vulnerable (citado por el 21%), seguido por los datos departamentales (18%). (Consulte la Figura 10).

FIGURE 10: Areas Most Vulnerable to Data Breaches or Incidents



Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

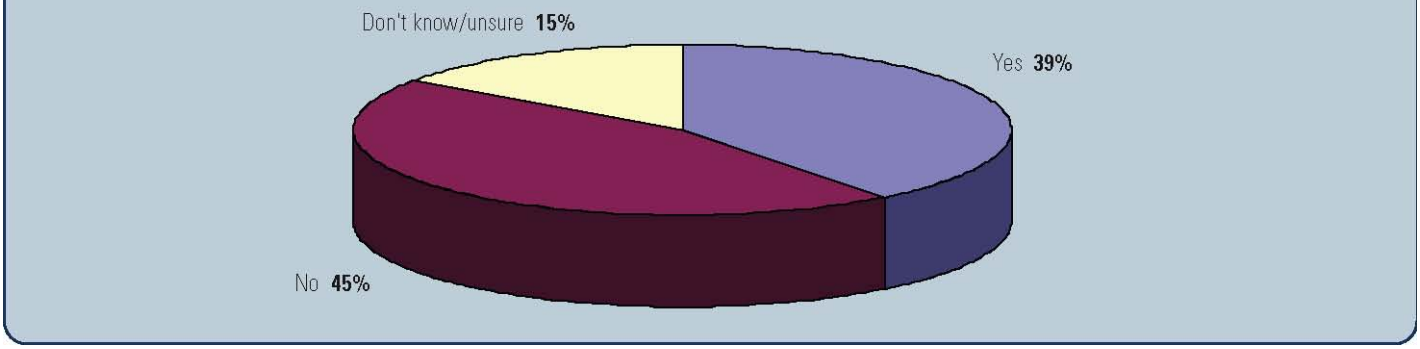
SUPERUSUARIOS

La mayoría de las organizaciones no ha implementado mecanismos para evitar que los administradores de bases de datos y otros usuarios de bases de datos con privilegios lean o alteren información delicada en aplicaciones financieras, de recursos humanos o en otras aplicaciones de negocios. La mayoría no puede ni siquiera detectar tales violaciones o incidentes.

Las violaciones de datos se pueden realizar por amplia variedad de usuarios dentro de la protección del cortafuegos corporativo. Usuarios internos, como administradores de bases de datos y sistemas, personal de desarrollo y pruebas, equipos de personal subcontratado y desarrolladores en otros países, pueden tener privilegios y acceder a información delicada en aplicaciones financieras, de recursos humanos, cuentas de clientes y otras aplicaciones. Menos de dos de cada cinco encuestados comentó que podía evitar tal alteración causada por superusuarios. (Consulte la Figura 11).

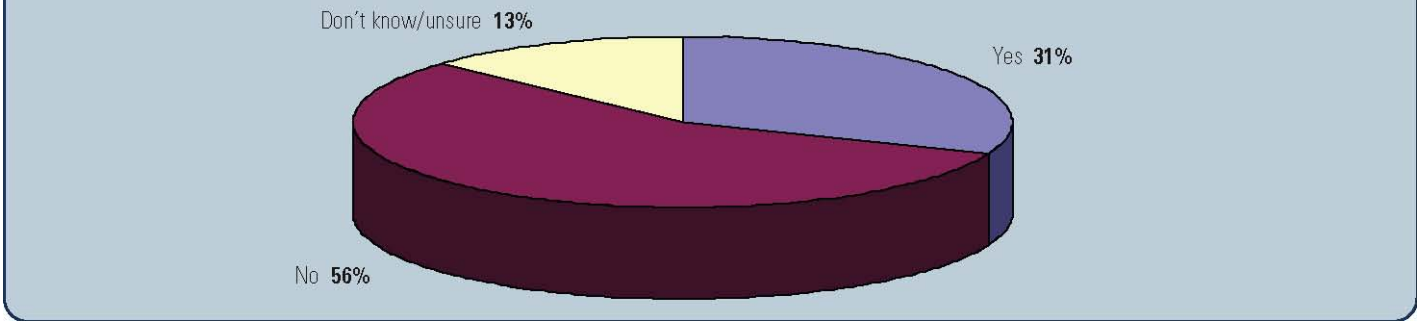
Evidentemente, muchas violaciones o incidentes con los datos son accidentes no intencionales y pueden ocurrir entre los superusuarios más precavidos. Sin embargo, la mayoría de las compañías de los encuestados no había iniciado acciones para evitar hechos accidentales. Sólo alrededor de un tercio informó de que tenía salvaguardas para evitar que un administrador de bases de datos moviera accidentalmente una tabla o causara de manera no intencional daños en bases de datos críticas para las aplicaciones.

FIGURE 11: Can Super Users be Prevented from Abusing Sensitive Data?



Sin embargo, otro tercio de los encuestados, un 31%, sostuvo que los usuarios pueden burlar aplicaciones y obtener acceso a sus datos en la base de datos directamente usando herramientas ad hoc. (Consulte la Figura 12). Y tal como observó uno de los encuestados: "Los usuarios con privilegios que tienen acceso a los datos a veces extraen información de sistemas desarrollados por los departamentos y manipulan los datos para generar informes. En ese punto, los datos están fuera de los niveles de control disponibles para asegurar su validez. Sin apoyo de los ejecutivos de nivel superior para detener este tipo de prácticas, no existe garantía respecto a la precisión de la información generada".

Figure 12: Can Users Bypass Applications and Access Application Data Directly Using Ad Hoc Tools?

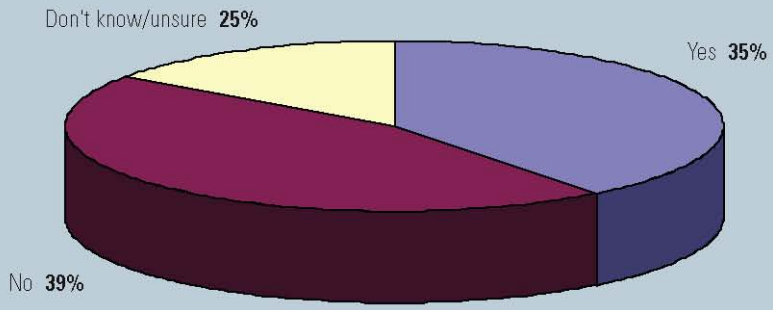


Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para consultar resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

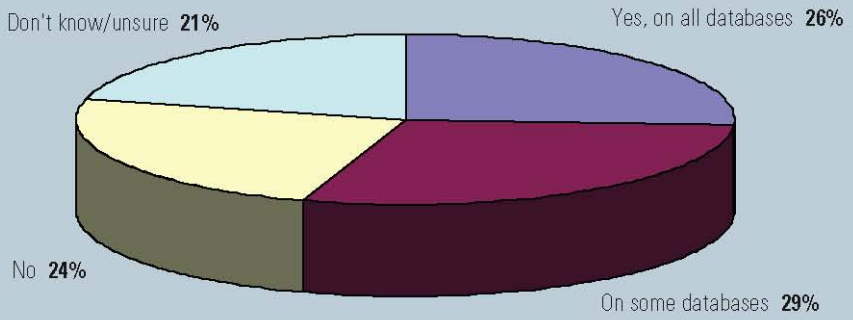
Algunas empresas han implementado capacidades de supervisión para ayudar a prevenir el posible abuso, ya sea intencional o no, de los superusuarios. Más de un tercio informó de que había comprobado que los administradores de bases de datos y otros usuarios con privilegios sobre las bases de datos en sus compañías no están abusando de sus privilegios de superusuarios. (Consulte la Figura 13).

FIGURE 13: Can Super-User Data Abuse be Monitored?



No obstante, la mayoría (un 55%), comentó que al menos algunos de los datos de auditoría de sus bases de datos estaban protegidos contra el acceso o la posible alteración de los usuarios de las bases de datos con privilegios. Sólo uno de cada cuatro pudo afirmar que esto se extiende a toda su cartera de bases de datos. (Consulte la Figura 14).

FIGURE 14: Is Database Audit Data Protected from Super-User Data Abuse?



Finalmente, sólo uno de cada 10 encuestados (un 9%) indicó que los administradores de bases de datos y otros usuarios de bases de datos con privilegios de su compañía había usado indebidamente, en algún momento, sus privilegios de superusuario para acceder a datos delicados. Y lo que es más contundente, cerca de la mitad de los encuestados del estudio, un 44%, informó de que simplemente no sabía si habían ocurrido tales violaciones.

Los elevados privilegios de los que disfrutan los superusuarios pueden ser el talón de Aquiles más frustrante de los esfuerzos para garantizar la seguridad de los datos. Es necesario que las compañías puedan examinar a estos usuarios y a los que trabajan en los sitios de sus socios y que, de la misma forma, tengan la capacidad de asegurar que estos usuarios sean conscientes de los estándares y protocolos de seguridad de datos y que se adhieran a ellos. Y aplicando el adagio "confíe, pero verifique", las organizaciones necesitan asegurarse de que las actividades de estos usuarios puedan ser verificadas nuevamente por otros profesionales.

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

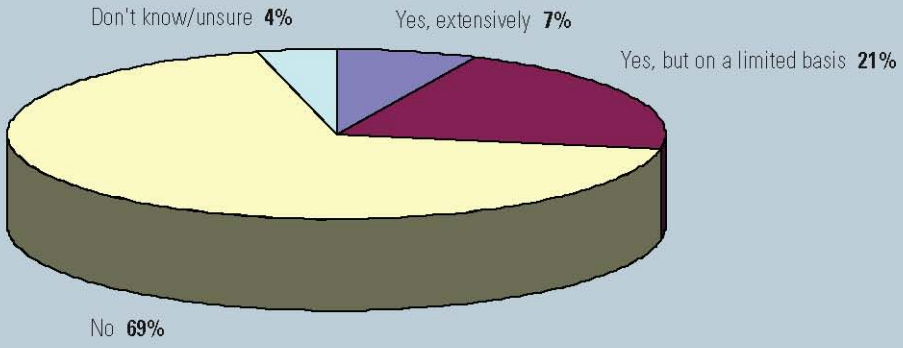
DATOS FUERA DE LAS INSTALACIONES

Enviar datos a partes externas es ahora una práctica común.

Otra vulnerabilidad de los datos, es el envío de ellos fuera de las instalaciones. Con la tendencia actual al crecimiento de la "empresa extendida", que depende de redes de socios, proveedores y clientes, es inevitable que los datos salgan más allá del cortafuegos. Las organizaciones están bajo una enorme presión para lograr mantener los centros de datos y las operaciones de las bases de datos trabajando las 24 horas al día, los 7 días de la semana. La encuesta reveló que muchas compañías habían recurrido a proveedores externos de servicios especializados que ofrecían servicios de administración y desarrollo. Tales proveedores asumen la responsabilidad de muchas de las tareas de bajo nivel o repetitivas para las cuales las empresas carecen de recursos de soporte.

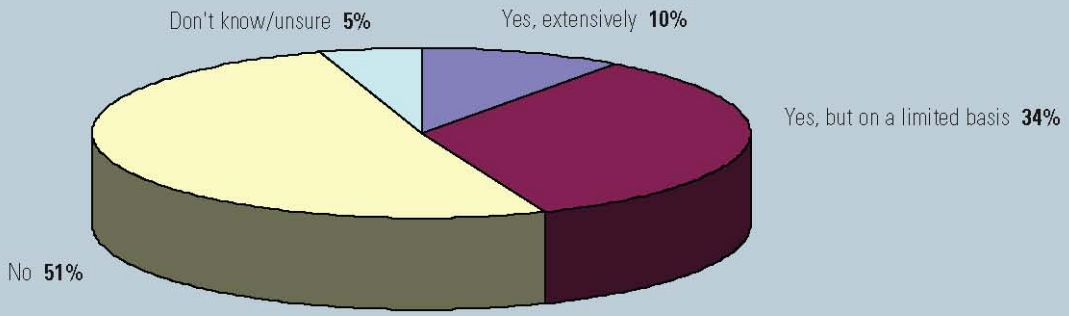
La subcontratación, por ejemplo, es una práctica que se está extendiendo a la administración de bases de datos. Alrededor del 28% de los encuestados informó de que sus organizaciones subcontratan o contratan en el extranjero al menos algunas de sus funciones de administración de bases de datos. (Consulte la Figura 15).

FIGURE 15: Are Database Administration Functions Outsourced?



Otro 44% comentó que subcontrata o contrata en el extranjero las funciones de desarrollo o prueba de bases de datos. (Consulte la Figura 16). Otro 34% informó de que enviaba backups o exportaciones de bases de datos no encriptadas fuera del sitio, a lugares como instalaciones de almacenamiento, socios de negocios u otros centros de datos. (Consulte la Figura 17).

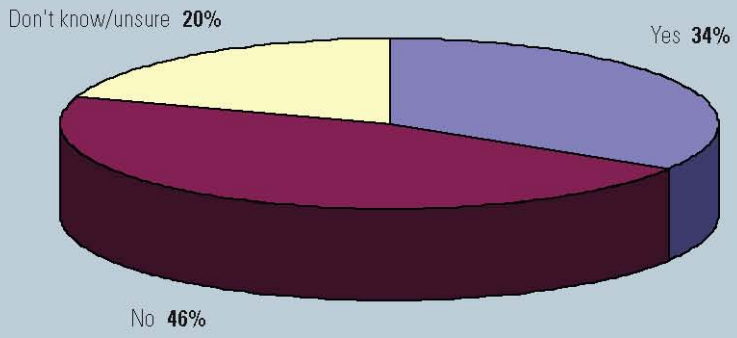
FIGURE 16: Outsource or Offshore Database Development or Test Functions?



Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

FIGURE 17: Are Unencrypted Database Backups or Exports Sent Offsite?



El desafío es que pocas compañías tienen certeza respecto de cuán seguros son sus datos y cuán bien los proveedores de servicio están cumpliendo incluso requisitos mínimos para la seguridad de los datos y el cumplimiento de normativas. Muchos proveedores de servicios terminan manejando datos delicados fuera de las instalaciones, sin ninguna de las salvaguardas que puede haber implementado la empresa original.

Tal como uno de los encuestados hizo notar: "las pruebas de recuperación ante desastres de los sitios de su compañía no incluyen procedimientos bien documentados de limpieza de datos". Y agregó que también estaba observando problemas de seguridad de datos similares con la desmantelación de servidores "que pueden no incluir la limpieza de los datos de los discos".

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para consultar resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

PROBLEMAS DE ENCRIPTACIÓN DE DATOS

Uno de cada cuatro sitios incluidos en esta encuesta no encripta los datos dentro de sus bases de datos y cerca de uno de cada cinco ni siquiera está seguro de si se realiza esta encriptación.

¿Cuán importante es la encriptación? Consideremos un caso reciente en que fue robada una computadora portátil del automóvil de uno de los proveedores de una compañía de alta tecnología; el equipo contenía datos personales delicados y no encriptados de 51.000 empleados actuales y anteriores de la compañía, incluidos nombres, números de la seguridad social, direcciones postales y detalles de derechos sobre acciones de la empresa y otras compensaciones de tipo accionario. Por desgracia, incidentes como éstos ocurren casi todas las semanas.

Reconociendo amenazas potenciales como ésta, alrededor del 57% de los encuestados de este estudio informó de que encriptaba al menos parte de la información de identidad personal de sus bases de datos, como los números de la seguridad social y de las tarjetas de crédito, al trasladarla a almacenamiento en disco. Sin embargo, es notable que el 43% no encripte dichos datos, o simplemente no sepa qué se está haciendo. (Consulte la Figura 18). La encuesta también descubrió que las prácticas de encriptación están mucho más avanzadas en las organizaciones más grandes (con más de 10.000 empleados) que en las más pequeñas. (Consulte la Figura 19).

FIGURE 18: Percentage of Companies Encrypting Personal Identity Information on Disks

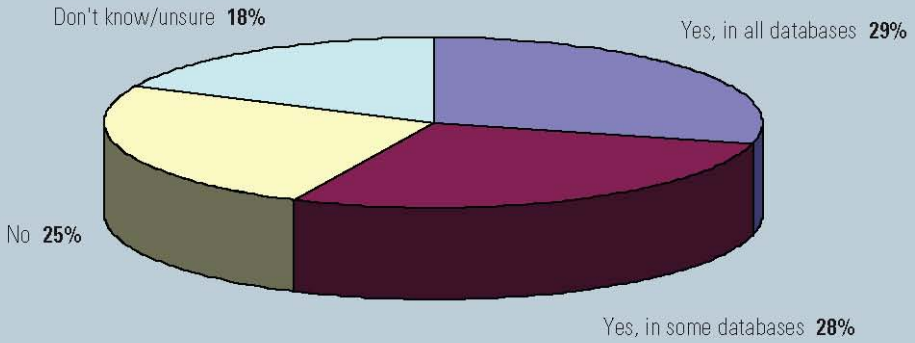


FIGURE 19: Percentage of Companies Encrypting Personal Identity Information on Disks--By Company Size

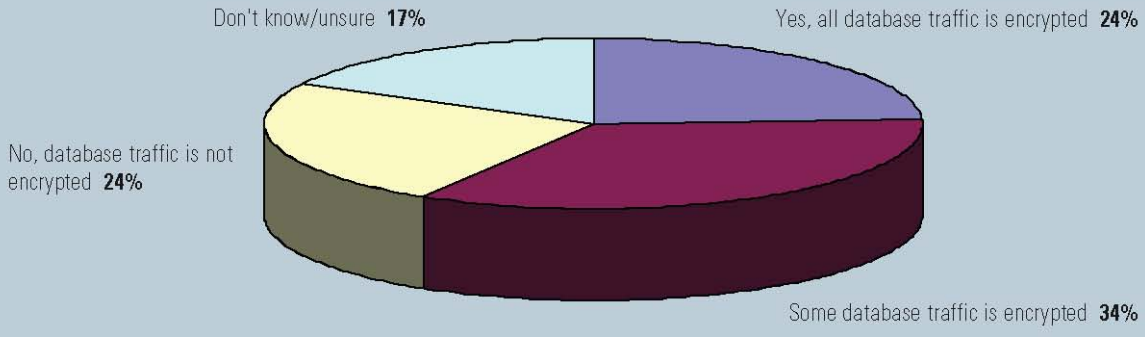
	Small	Medium	Large
Yes, in all databases	28%	19%	41%
Yes, in some databases	22%	36%	26%

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

De manera similar, el 41% no encripta o no sabe si encripta, los datos de las aplicaciones de la red, que ingresan o salen de sus bases de datos. (Consulte la Figura 20). La encuesta también reveló que el 34% envía con conocimiento, backups o exportaciones de bases de datos no encriptados fuera del sitio a instalaciones de almacenamiento, socios de negocios u otros centros de datos.

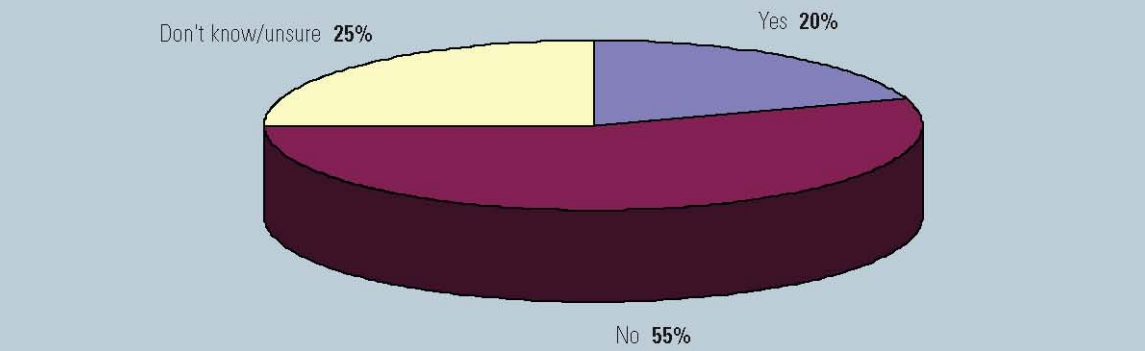
FIGURE 20: Is Application Data Encrypted on the Network to/from Databases?



Un encuestado citó "el uso de dispositivos no autorizados para la transferencia de datos como unidades de memoria USB, discos duros portátiles, etc. donde no hay certeza de que los datos estén encriptados y que sean indescifrables, en particular cuando estos medios se pierden o son robados.

Sólo uno de cada cinco encuestados encripta todos sus backups y exportaciones de bases de datos en línea y fuera de línea. (Consulte la Figura 21).

FIGURE 21: Are All Online and Offline Database Backups and Exports Encrypted?



Hasta cierto grado, es posible que se requiera capacitación y formación para implementar con mayor efectividad medidas de encriptación de datos. Uno de los encuestados comentó que "los desarrolladores pueden actualizar una base de datos en el momento en que lo deseen y que no serían capaces de comprender las herramientas de encriptación".

La encriptación de datos es una solución técnica sostenible para los dilemas de envío de datos a ubicaciones fuera del sitio, ya sea para almacenamiento o para probar nuevas aplicaciones.

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

PRUEBAS DE DATOS DELICADOS

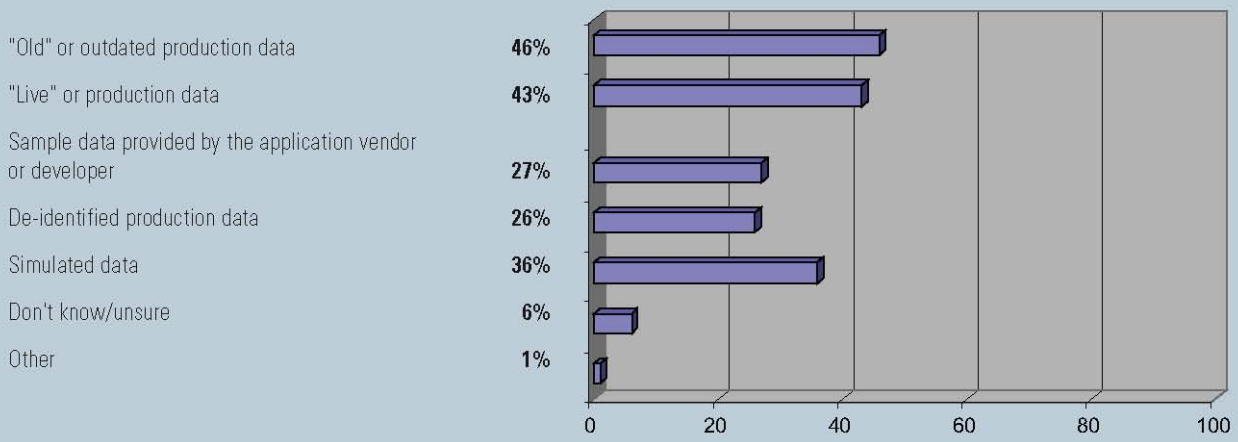
Dos de cada cinco organizaciones emplean datos de producción reales dentro de entornos que no son de producción, con lo cual exponen esta información en entornos sin seguridad.

Las empresas tienden a ser más complejas y a tener muchas aplicaciones aisladas. En consecuencia, cuatro de cada 10 encuestados informó de que no conocía todas las bases de datos dentro de sus organizaciones que contenían información delicada, como números de tarjetas de crédito de clientes o datos de los socios.

Otro problema que afecta a la seguridad de los datos es el manejo de datos en vivo dentro de entornos que no son de producción, como los de prueba y puesta en marcha de aplicaciones. Para agilizar los procesos, muchos departamentos de IT mueven muestras de datos fuera de producción a estos entornos, suponiendo que dado que están fuera de línea, están protegidos contra amenazas maliciosas. Sin embargo, dentro de estos entornos, los usuarios internos no autorizados pueden acceder a los datos. Como se mencionó anteriormente, el porcentaje de compañías que tienen salvaguardas contra las violaciones o incidentes tanto intencionales como no intencionales causados por "superusuarios" internos es muy reducido.

Más de dos de cada cinco encuestados sostuvo que los datos de producción en vivo se mueven por lo general a entornos que no son de producción para procesos fuera de línea, como los de prueba o entornos de preproducción y desarrollo. (Consulte la Figura 22). Es incluso más alarmante que más de un tercio de los datos que se mueven fuera de línea contengan información delicada como números de tarjetas de crédito, números de la seguridad social o información identificable de clientes, socios o empleados. (Consulte la Figura 23).

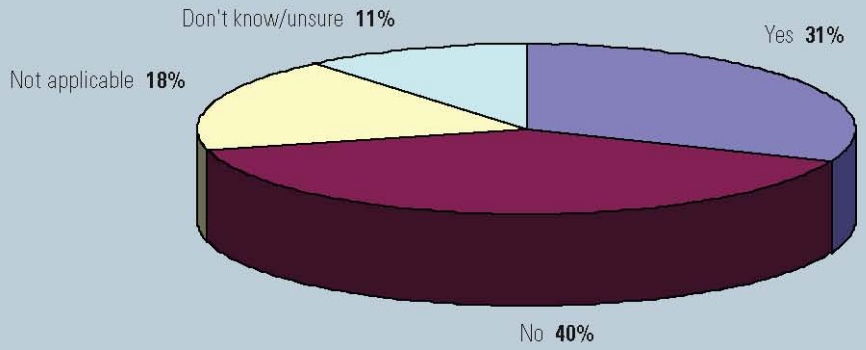
FIGURE 22: Types of Data Used Within Non-Production Environments



Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

FIGURE 23: Percent of Companies Shipping Unencrypted Production Data Containing Sensitive Data



Pero no sólo el empleo de datos de producción para pruebas representa un problema frustrante para los encuestados, sino que también las nuevas iniciativas para entornos replicados o de alta disponibilidad están creando problemas para la seguridad de los datos. "La exportación temporal de datos para pruebas y desarrollo hace que los datos permanezcan en almacenamiento local en equipos de escritorio", comentó un encuestado. "También tenemos transmisión de datos a destinos débilmente resguardados como parte de entornos de replicación o de alta disponibilidad".

Pese a que el 27% de los encuestados indicó que los datos son "desidentificados" antes de moverlos a entornos que no son de producción, sólo un cuarto de ellos puede afirmar que hay implementado un procedimiento sistemático para asegurar que esta desidentificación se realiza en todos los casos.

Los departamentos de IT prefieren trabajar con datos reales cuando prueban o desarrollan nuevas aplicaciones para simular tan fielmente como sea posible los casos de uso reales. Sin embargo, las empresas necesitan asegurar de mejor forma que se haya eliminado de estos datos cualquier identificador que pueda exponer datos delicados de clientes o socios.

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

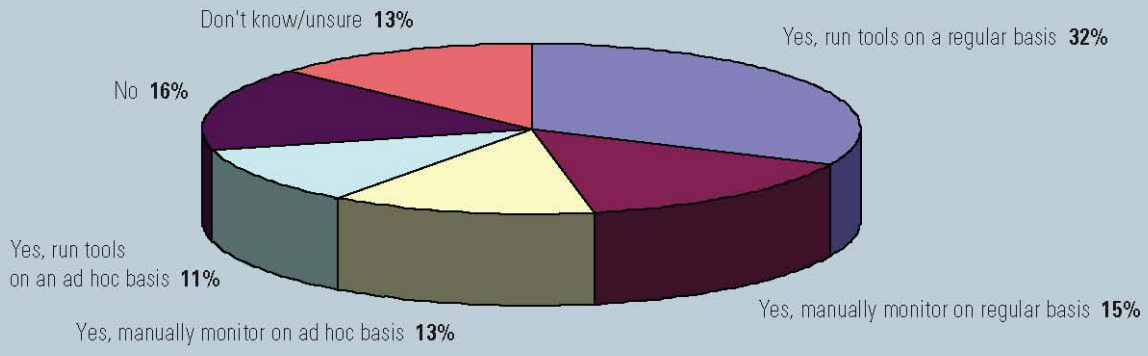
Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

SUPERVISIÓN Y AUDITORÍA

Existe una creciente conciencia con respecto a los riesgos potenciales. La mayoría de las organizaciones supervisa sus bases de datos en busca de cambios que puedan ser indicadores de actividad maliciosa.

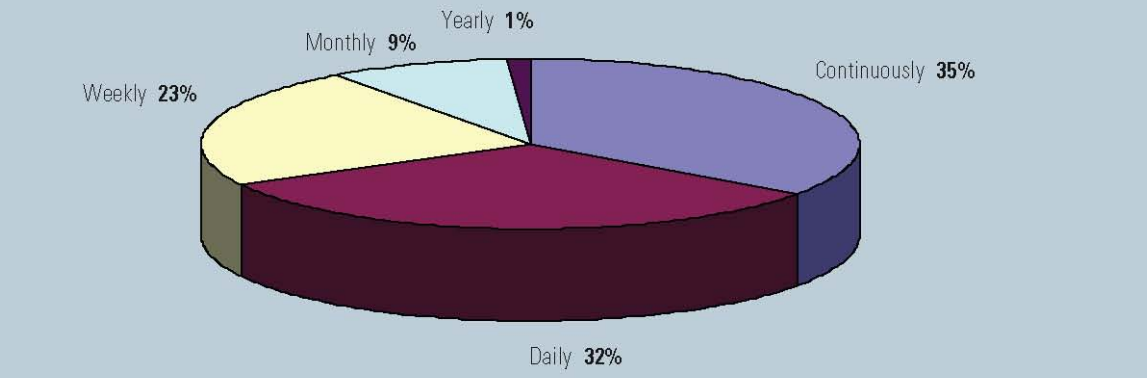
Pese a que gran parte de este informe analizó los numerosos riesgos y vulnerabilidades a los que las empresas siguen exponiendo sus datos corporativos, también hay buenas noticias. La encuesta descubrió que la mayoría de las organizaciones había intensificado sus esfuerzos de supervisión para mejorar las instancias de detección de violaciones de datos. Por ejemplo, más de siete de cada 10 encuestados manifestó que actualmente estaba supervisando sus bases de datos de producción en busca de problemas de seguridad o cambios en la configuración. Un total del 44% informó de que este proceso es ad hoc, mientras que el 47% comentó que captura dicha información regular y sistemáticamente, ya sea ejecutando herramientas automatizadas o mediante revisiones manuales periódicas. (Consulte la Figura 24).

FIGURE 24: Currently Monitoring All Production Databases for Security Issues or Configuration Changes?



La mayoría de las organizaciones que supervisan sus bases de datos de producción lo hacen para capturar datos dentro de un período de 24 horas. Más de un tercio, un 35%, indicó que esta supervisión era continua, mientras que el 32% informó de que hacía actualizaciones diarias. (Consulte la Figura 25).

FIGURE 25: If Regularly Monitoring Production Databases, How Often?

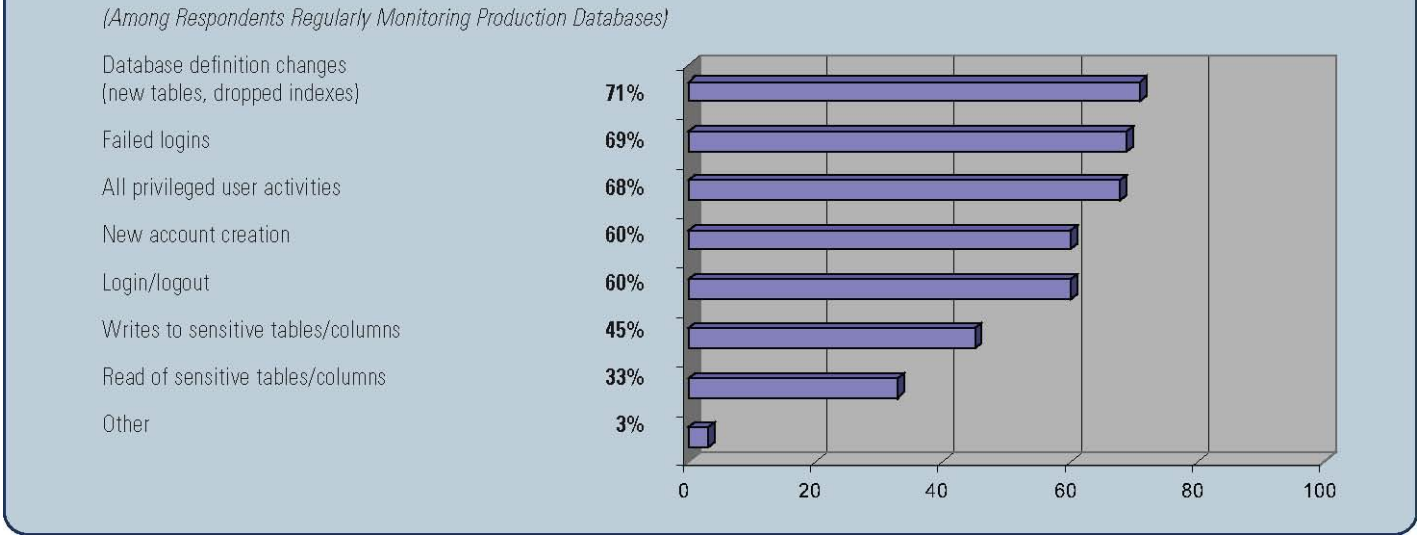


Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

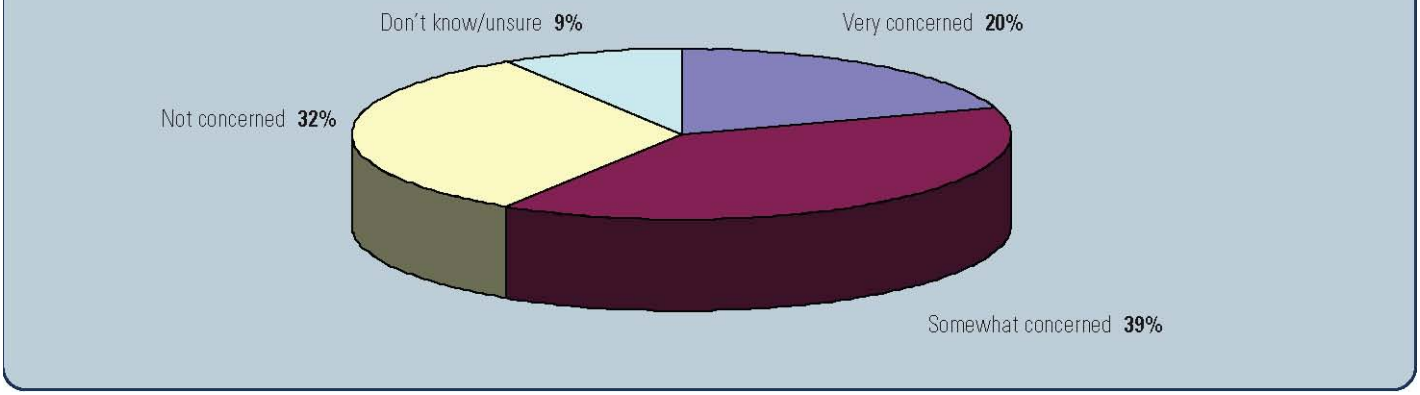
Entre quienes respondieron que supervisaban sus bases de datos de producción, siete de cada 10 encuestados indicó que buscaba cambios en la definición de las bases de datos, como nuevas tablas o índices movidos, o evidencia de inicios de sesión fallidos. Al menos el 68% vigilaba las actividades de los usuarios con privilegios. (Consulte la Figura 26).

FIGURE 26: Activities Regularly Monitored



Ante tanta atención para detectar violaciones importantes de las bases de datos y con regulaciones estatales, federales e industriales que obligan a las organizaciones a hacerse responsables de salvaguardar mejor los datos, existe un creciente énfasis en la auditoría de las bases de datos. Seis de cada 10 encuestados afirmó que estaba preocupado por la capacidad de sus organizaciones para aprobar las auditorías que requieren demostrar el cumplimiento de las regulaciones sobre protección de datos. (Consulte la Figura 27).

Figure 27: Percent of Respondents Concerned About Data Compliance Audits



Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

Siete de cada diez encuestados informó de que usa la auditoría de base de datos nativa para supervisar las actividades en las bases de datos. La mayoría de los encuestados, un 53%, comentó que "toma unos cuantos días" prepararse para una evaluación/auditoría de seguridad de las bases de datos. Cerca de uno de cada cuatro incluso manifestó que puede prepararse en horas, lo que sugiere que se han implementado procesos sistemáticos o incluso automatizados para manejar dichas tareas.

Más de dos quintos, un 42%, indicó que podía detectar y corregir un cambio no autorizado en una base de datos en 24 horas. Un poco más de la mitad, un 51%, sostuvo que sabría si alguien hiciera un cambio no autorizado en la configuración en la mayoría de las bases de datos de su organización. Un total de un 84% se enteraría de cambios no autorizados en al menos algunas bases de datos de su organización.

CONCLUSIÓN

La seguridad de IT y de los datos sigue estando muy arriba en las listas de las prioridades corporativas. Sin embargo, pese a que las compañías son conscientes y han estado trabajando agresivamente para proteger las bases de datos contra el hackeo externo, la mayoría no ha abordado por completo amenazas que no se ven o que pasan desapercibidas relacionadas con la exposición de los datos a violaciones internas.

Menos de dos de cada cinco encuestados comentó que puede evitar alteraciones de los superusuarios y sólo un tercio informó de que tenía salvaguardas para evitar que el administrador de una base de datos moviera por accidente una tabla o causara sin querer daños en bases de datos críticas para las aplicaciones.

Además, muchos datos se envían fuera de las instalaciones y lejos del control de la empresa. Alrededor del 27% de los encuestados informó de que sus organizaciones subcontrataban o contrataban en el extranjero al menos algunas de las funciones de administración de bases de datos y otro 44% manifestó que subcontrataba o contrataba en el extranjero funciones de desarrollo o prueba de bases de datos. Otro 34% informó de que enviaba backups o exportaciones de bases de datos no encriptadas fuera del sitio, a lugares como instalaciones de almacenamiento, socios de negocios u otros centros de datos.

La encriptación puede abordar algunas de las vulnerabilidades. Alrededor del 57% de los encuestados informó de que encriptaba al menos parte de la información de identidad personal de sus bases de datos, como los números de la seguridad social y de las tarjetas de crédito, al trasladarla a almacenamiento en disco. Sin embargo, es notable que el 43% no encripte dichos datos o simplemente no sepa qué se está haciendo. Uno de cada cuatro encuestados no encripta ningún dato de las aplicaciones de la red al entrar o salir de sus bases de datos y el 34% envía con conocimiento backups o exportaciones de bases de datos no encriptados fuera del sitio a instalaciones de almacenamiento, socios de negocios u otros centros de datos.

Más de dos de cada cinco encuestados sostuvo que los datos de producción en vivo se mueven por lo general a entornos que no son de producción para procesos fuera de línea, como los de prueba o entornos de preproducción y desarrollo. Más de un tercio de los datos que se mueven fuera de línea contienen información delicada como números de tarjetas de crédito, números de la seguridad social o información identificable de clientes, socios o empleados.

Hay importantes vacíos en la seguridad de los datos que pueden exponer información delicada ante las personas equivocadas, ya sea detrás del cortafuegos de la empresa o en las instalaciones de los socios. Muchas empresas han tenido éxito en salvaguardar sus bases de datos contra intrusos externos, pero se requiere más trabajo para proteger con efectividad estos datos contra riesgos más cercanos.

Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

ASPECTOS DEMOGRÁFICOS

FIGURE 28: Number of Databases at Respondents' Companies

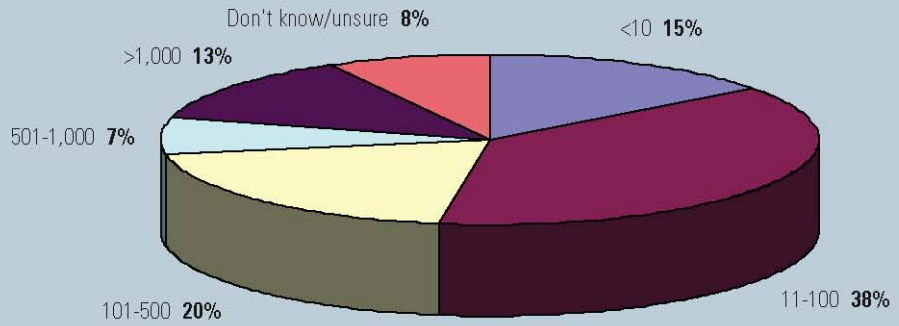
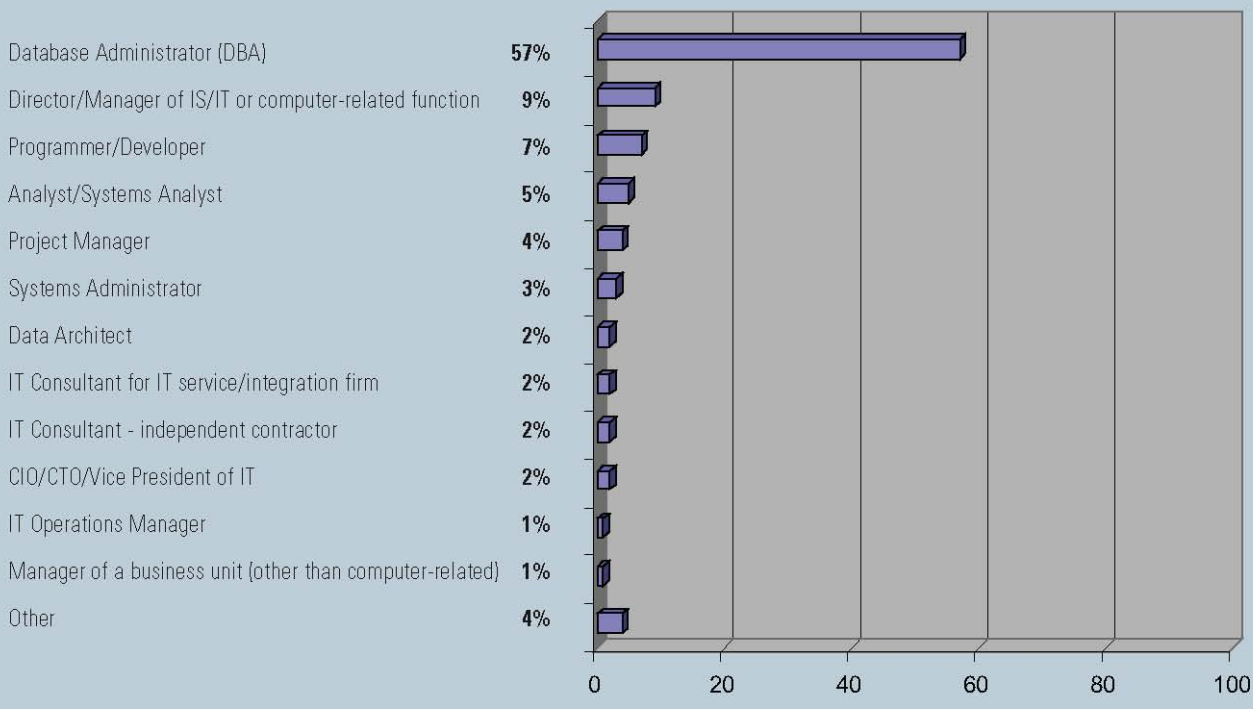


FIGURE 29: Respondents' Primary Job Titles



Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para leer resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

FIGURE 30: Respondents' Companies by Number of Employees

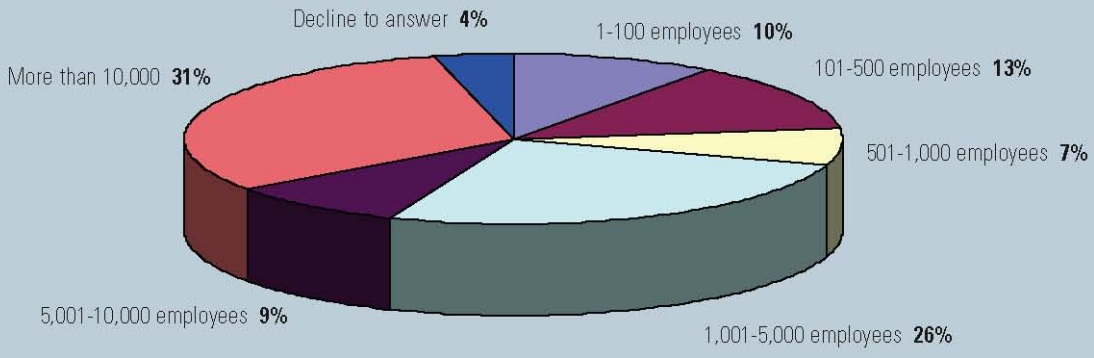
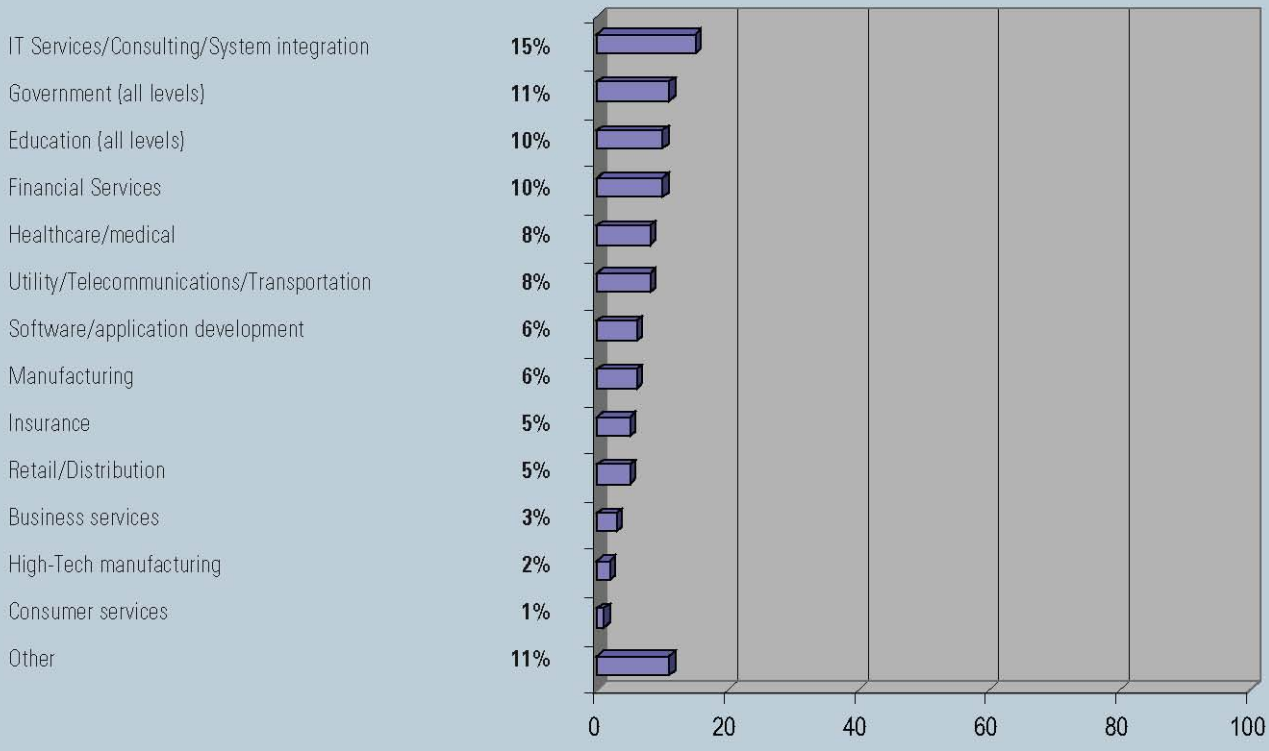


FIGURE 31: Respondents' Primary Industries



Inseguridad de los datos empresariales: ¿Están preparadas las organizaciones para enfrentar amenazas internas? está auspiciado por ***Oracle*** y producido por ***Unisphere Research***. Unisphere Research es la unidad de investigación de mercado de Unisphere Media, una división de Information Today, Inc. Para consultar resúmenes de nuestros informes anteriores, visite www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, correo electrónico: Tom@dbta.com. Web: www.dbta.com

Participe en IOUG: si aún no es miembro de IOUG y desea continuar recibiendo información clave como ésta, visite IOUG en w3.ioug.org/join/today y obtendrá información sobre cómo unirse a esta dinámica comunidad de usuarios para profesionales de la tecnología y bases de datos Oracle.

La información contenida en el presente informe ha sido recopilada a través de encuestas basadas en Web de listas de miembros y posibles miembros proporcionadas por IOUG, mediante entrevistas con participantes con conocimientos en la industria de la computación y a través de investigación secundaria de documentos, informes y otros medios publicados generalmente disponibles, así como de estudios anteriores realizados por Unisphere Research. Unisphere Research ha confiado en la precisión y validez de toda la información obtenida. Unisphere Research no asume responsabilidad por informaciones imprecisas u omisiones.

Unisphere Research no será responsable por errores en el documento, sus datos y análisis ni por daños incidentales o consecuentes en conexión con el uso de este documento y su información.

La recopilación y el análisis de los datos fueron realizados con SurveyMethods.