PowerData

Especialistas en Gestión de Datos

Seguridad de datos

Del firewall al cloud. De la confianza al ahorro

ÍNDICE

Seguridad de datos
Del firewall al cloud. De la confianza al ahorro

> Sólo en España, el coste de los ataques a la información ascendió a 14.000 millones de euros el pasado año.

NAE

Una de las preocupaciones clave para la mayoría de organizaciones es la seguridad de sus datos. Planes, estrategias, presupuestos... cada año, **la inversión destinada a proteger la información aumenta, pero estos esfuerzos no siempre están bien dirigidos.**

¿Es lo mismo proteger un entorno real que uno de pruebas? **¿Puede programarse la seguridad en cloud igual que en un entorno on premise? ¿Cuál es la tecnología más efectiva?**

Lo cierto es que, **el balance de este año deja bastante que desear y las cifras demuestran que aún queda mucho por recorrer** para poder garantizar una seguridad efectiva:

- Las compañías no se ocupan lo suficiente de los privilegios de los administradores ni de la dispersión de los datos algo que, para el 81% de los encuestados, supone una amenaza "muy importante" o "importante" (*KuppingerCole*).
- El 68% de las compañías tiene dificultades para restringir el acceso de los usuarios a los datos sensibles (*Ponemon*).
- El 69% de los responsables de la toma de decisiones todavía ven la seguridad de datos como una carga, en términos de tiempo y presupuesto y, sin embargo únicamente el 18% de ellos confía plenamente en que sus datos están seguros cuando los empleados acceden remotamente, según un reciente *estudio*.
- El 67% de las compañías percibieron niveles severos o altos de amenaza hacia sus sistemas de control, frente al 43% de 2015 (*Sans*).
- El 91% de las empresas son vulnerables ante diferentes tipo de ataques a su información ().

Por suerte, siempre estamos a tiempo de hacer mejor las cosas. Aún no es tarde y así lo demuestran algunos cambios que indican que la t**endencia es reforzar la seguridad**:

- **El 70% usan servicios de seguridad basados en la nube y el 51% actualmente emplean análisis de grandes datos para modelar e identificar incidentes de seguridad de la información** (*IDG*).
- **El 56% de los encuestados trasladan datos confidenciales a la nube, cifrados o protegidos por técnicas como el enmascaramiento de datos;** el 17% de ellos protegen sus datos en reposo en cloud de la misma forma **y el 28% esperan hacerlo en los próximos dos años** (*Ponemon*).
- **El enmascaramiento de datos es una de las opciones mejor valoradas, como así demuestra su popularidad entre las empresas Fortune 500.** Un ejemplo es que, entre los usuarios de LastPass, un servicio que enmascara las contraseñas, se encuentran más de 10.000 clientes corporativos que incluyen a muchas de estas compañías, según declara Cid Ferrara en *CSO*.

¿Están los datos de tu negocio protegidos? Si has comprado espacio de almacenamiento adicional, cuentas con demasiados activos de TI obsoletos, has experimentado recientemente una pérdida de datos o tu presupuesto para la gestión de la información no ha aumentado en el último año, deberías plantearte el **actualizar tu estrategia de protección de datos.**

Todos somos responsables de la seguridad de datos, a todos nos afecta la falta de protección y tú decides cuándo y por dónde empezar.

> Las pérdidas financieras estimadas como resultado de todos los incidentes de seguridad aumentaron en un 159%, con respecto al año anterior.

PricewaterhouseCoopers "Global Information Security Survey 2016

La seguridad de datos en el cloud

¿Tienes la certeza de que la información que tu negocio almacena en la nube está segura? Lo cierto es que el **cloud entraña más riesgos que los entornos tradicionales** suponiendo un desafío, todavía mayor para empresas que trabajan con información sensible, como pueden ser las compañías del sector seguros, las de la salud o las entidades financieras.

La seguridad en la nube debe ser considerada de forma distinta a la protección de datos on premise. Pero no hay que retrasar más el momento de diseñar un plan de seguridad con este propósito, porque:

1. **El número de usuarios de la nube personal aumenta cada año:** el correo electrónico, los CDs y las memorias USB se han visto sustituidas por aplicaciones basadas en la nube, que permiten intercambiar información de forma fácil y sencilla y guardar de forma permanente imágenes, vídeos, tablas Excel o archivos de texto.

2. **El uso de la nube trasciende a otras esferas: porque a pesar de las dudas, la confianza en el cloud no deja de aumentar.** Documentos con información confidencial, papeles del banco, facturas... todo pasa por la nube.

3. **Intercambio de datos en las altas esferas:** la colaboración entre empresas, que refuerza los vínculos entre proveedores, clientes y socios, entre otros; también se apoya en el cloud para mantener un flujo de información continuamente accesible, de forma práctica y cómoda.

Pero, a pesar de todo, no todo el mundo está seguro de que su información está protegida.

Las razones son muchas, pero cabe destacar:

a) **Legislación: es imposible para los diferentes ordenamientos jurídicos adaptarse a la realidad al ritmo al que avanza la tecnología.** La legislación sobre privacidad de datos se desarrolla de forma reactiva y desigual, existen muchas propuestas y, al final, puede contarse **con muy poco desarrollo normativo en firme.** El motivo es que, primero sorprenden las novedades que van apareciendo en este ámbito y, a continuación, se regula. Pero, además, **cada país lo hace a su manera. No existen normas universales o leyes que puedan ser aplicables a cualquier usuario y cualquier servicio en la nube**, independientemente de los límites geográficos o la residencia y esto es un problema.

b) Servidores: una de las cuestiones que más complican la normalización del cloud son los servidores. Aumentan los ejemplos de éxito en la regulación de los problemas de privacidad de los datos almacenados en los servidores dentro del propio país y, sin embargo, existe **un gran vacío legal en lo referente a los flujos transfronterizos de datos**. Es complicado determinar a quién corresponde ocuparse de legislar cuando el servidor se aloja en una determinada localización, que no corresponde con el país de procedencia ni residencia del usuario propietario de esa información y tampoco lo hace con los países por los que los datos circulan en su tránsito desde que abandonan el ordenador del usuario y hasta que llegan a su destino, el servidor en la nube.

c) Acceso: determinar quién puede obtener permiso legal para acceder a los datos almacenados en la nube y en qué supuestos está autorizado a hacerlo no resulta nada sencillo. Mientras que los espacios de almacenamiento en la nube funcionan bajo sus propias reglas (en el mejor de los casos), los usuarios creen que su información es confidencial y está a salvo de intrusos. Y esto no funciona así, porque **aunque esos datos sean de su propiedad, el espacio donde los almacenan no pertenece a ellos.**

En cualquier caso, se sea más o menos consciente de la problemática que rodea a la falta de reglas en el uso de la nube, es muy recomendable tratar de mejorar la propia experiencia. Para ello, la prioridad es ocuparse de la seguridad y, para lograr una protección más efectiva de los datos en la nube es recomendable:

1. Restringir su uso a materias menos comprometidas

Mientras que no existan mayores garantías, no merece la pena almacenar información confidencial en la nube. Se puede optar por conservar los datos más sensibles en entornos locales y otros tipos de información en el cloud. Hacer esta diferenciación es una buena forma de comenzar a perder el miedo al cloud, sin riesgos y aprovechando todas sus ventajas para el negocio.

2. Saber elegir proveedor cloud

La nube no es una, sino que podría decirse que existen tantos clouds como proveedores. Por eso, antes de firmar un contrato y enviar a la nube los valiosos activos informacionales de la organización, merece la pena leer el acuerdo de usuario para averiguar cómo funciona el servicio de almacenamiento en la nube. Es preferible invertir un poco de tiempo al principio, que sorprenderse después, cuando ya es demasiado tarde para remediar el desastre.

3. Reforzar la autoprotección

Existe una única ocasión de blindar una cuenta por parte del propio usuario. Es el momento de decidir la contraseña y, pese a que la preocupación por la seguridad va en aumento, la mayoría de las personas pasan por alto este tipo de oportunidades de ganar en seguridad. Hay que dejar de usar las mismas claves para todo, de no combinar mayúsculas y minúsculas, de olvidarse de incluir caracteres numéricos y de no tomarse en serio la protección de las cuentas, desde la de correo electrónico a la de la banca online.

4. Encriptar los datos

El cifrado es, hasta ahora, la mejor manera de proteger los datos. Interesa tener la seguridad de que, caso de que todo falle, se produzca la brecha de seguridad y personas no autorizadas accedan a la información....ésta no les servirá de nada. La encriptación es el único medio de conseguirlo y hay que plantearse esta opción a la vez que se plantee la migración a un entorno cloud.

5. Buscar la encriptación de serie en la nube

Los proveedores cloud, conocedores de la inquietud de sus clientes y usuarios acerca de la seguridad de su información, han comenzado a ofrecer servicios de encriptación local y descifrado de archivos, además de almacena-

miento y copia de seguridad. Esto significa que el servicio se encarga de cifrar los archivos en el ordenador del usuario, para después almacenarlos de forma segura en la nube.

No todos los datos son iguales y no todos necesitan el mismo nivel de protección. Es necesario conocer los activos informacionales de la organización, para poder determinar el nivel de privacidad que necesitan y definir las medidas de protección más adecuadas. La inversión consciente siempre es rentable. No hace falta encriptar todos los archivos de la compañía, pero puede ser la mejor solución para ésos que contienen información sensible. ¿Ya sabes cuáles son? ¿Puedes alcanzar el equilibrio entre el nivel de protección requerido y el tiempo y recursos invertidos?

Acciones para promover la seguridad de datos

> Mientras que los registros de empleados y clientes siguen siendo los principales objetivos de los ciberataques, el daño a la marca y la reputación aumentó hasta alcanzar un 72% en 2015.
>
> *PricewaterhouseCoopers "Global Information Security Survey 2016*

La protección de los datos es una responsabilidad del negocio y lo es tanto desde el punto de vista de la ética, como desde el del cumplimiento. Para actuar correctamente **hay que diferenciar la promoción de la seguridad en entornos locales y en la nube**. De esta forma, es más sencillo **diseñar un plan efectivo** para ganar esa tranquilidad que da el tener el control.

Seguridad de datos en la nube

Para comenzar a planear una estrategia en la nube hay que pensar en el largo plazo y buscar la efectividad, sin temer al dinamismo de este entorno ni a la falta de regulación que lo define. A partir de ahí, se puede:

1. **Clasificar los datos corporativos: determinar qué datos son importantes y cuáles resultan menos relevantes, separar los más críticos de los demás y priorizar su gestión y control.** Es fundamental evitar estandarizar, ya que aplicar las mismas medidas de protección a todos los activos informacionales puede suponer quedarse corto en algunos casos y derrochar recursos en otros.
2. **Promover la integración:** cuando la información de la compañía está confinada y separada en distintos silos, cuando además no existe comunicación entre IT y el área de negocio, se corre un gran riesgo al plantearse iniciati-

vas como la nube. Hace falta **entender de qué datos dispone la organización, cómo se configuran y de qué modo evolucionan.** Llevar a cabo una adecuada gestión de la información es la única garantía que existe para entender cómo los controles de seguridad podrían afectar a la organización.

3. **Confiar sólo en los mejores:** no todas las nubes son iguales. En algunas existen normas y en otras no, unos proveedores cloud priorizan la seguridad de sus clientes y otros ponen el foco en otros aspectos del servicio. Teniendo en cuenta estas diferencias, hay que **hacer la mejor elección para no perder el control sobre los propios datos.**

Seguridad de datos en otros entornos

Nuevas posiciones, como el CISO, aumento en los presupuestos de seguridad…. y, a pesar de todo, las empresas todavía no están obteniendo los resultados esperados. Por una parte, el centrar toda su atención en el cloud y su estrategia no termina de favorecer a lo que sucede en entornos locales. Por otra, las organizaciones suelen cometer algunos errores que pueden costarles caros. Fallos que tienen que ver con:

1. **Adquirir los últimos lanzamientos en tecnología** independientemente de si tiene más o menos sentido para la estrategia de seguridad específica.
2. Obviar la necesidad de invertir en el desarrollo de capacidades avanzadas que ayuden a detectar atacantes, como el análisis de malware, la inspección del tráfico que sale de la red o el modelado de amenazas.
3. **No gestionar la seguridad** de forma efectiva, algo que se pone de manifiesto con la descompensación entre el programa de seguridad, sus resultados y la necesidad de personal que se ocupe de él.
4. **Faltarles talento.** Todavía es posible encontrar a los perfiles adecuados para el área de seguridad de la información. No hay que retrasar su búsqueda porque, si se deja para más adelante la inversión en este tipo de perfiles profesionales se llegará a un punto sin retorno, el de la **escasez del 47% en profesionales de la seguridad cualificados** que anuncia un reciente estudio.
5. **Olvidarse de desactivar las aplicaciones de seguridad obsoletas** o en desuso al adquirir nuevas.
6. Invertir en tecnología de seguridad sin disponer de la **experiencia**, las capacidades o el personal suficiente para mantener, o hacerlo sin tener en cuenta la necesidad de asignar un presupuesto para formación.
7. Centrarse en tecnologías defensivas para ocuparse de la seguridad y dejar de lado las que se ocupan de **dar respuesta a los incidentes.**

Además de evitar este tipo de errores, a nivel práctico, al afrontar la seguridad de datos en la empresa hay que tener en cuenta las siguientes recomendaciones:

a) **Garantizar la seguridad a nivel de usuario,** no sólo a nivel de dispositivos porque éstos ya tendrán su disponibilidad, su backup y su capacidad para proteger el dato en sí.

b) **Conocer qué datos necesitan ser protegidos de forma más especial.** Números de cuenta, DNIs, correo, email, tarjetas de crédito, direcciones… un análisis de la información proveerá de la respuesta en cada caso.

c) **No descuidar los ambientes no productivos** como los de desarrollo, capacitación o pruebas.

d) Tener en cuenta que, al aplicar algunas medidas de protección, como el enmascaramiento, el dato cambia, pero hay que **mantener la integridad referencial** en toda la base de datos, porque si no aparecen las inconsistencias y ya no sirven para entornos productivos.

e) **Darse cuenta de que, aunque enmascaramiento y encriptación se entienden como acciones equivalentes, en realidad no lo son.** El nivel de protección que proporcionan y el poder hacer reversible la acción son las principales diferencias entre ambas.

Mejores prácticas en seguridad de datos

> Las organizaciones detectaron un 154% más de incidentes en 2015 que el año anterior.
>
> *PricewaterhouseCoopers "Global Information Security Survey 2016*

El nivel de protección de la información de la organización puede aumentar cuando en el plan de seguridad se tienen en cuenta mejores prácticas como las siguientes:

1. **Definir una estrategia global de seguridad y actualizarla.**
2. **Monitorizar todas las aplicaciones con acceso a datos** para detectar las menos seguras y trabajar sobre esos puntos débiles, evitando que se conviertan en una puerta de acceso para los hackers.
3. **Crear controles de acceso específicos** para todos los usuarios, limitando su acceso a los sistemas que necesitan para sus tareas exclusivamente y, reduciendo así la exposición de los datos sensibles.
4. **Obtener un registro completo y detallado de lo que ocurre en los sistemas corporativos.** Una decisión que, además de reforzar la seguridad, facilitará la resolución de problemas.
5. **Asegurarse de que la seguridad del software y del hardware están actualizadas** con las nuevas tecnologías antimalware.
6. **Nombrar a un CISO** para que se haga cargo de la seguridad.
7. **Formar a los usuarios** en mejores prácticas de seguridad cibernética para que sepan crear contraseñas seguras, reconocer emails sospechosos de amenaza, evitar aplicaciones peligrosas y prevenir cualquier otro riesgo relevante para la seguridad de la información.

8. **Definir claramente los requisitos y las expectativas** de la organización en materia de seguridad, especialmente al practicar contrataciones o al iniciar relaciones con socios y proveedores.
9. **Determinar una línea de base que incluya los estándares de seguridad** aplicables a terceros.
10. **Monitorizar la actividad usuaria** para verificar que sus acciones cumplen con las recomendaciones de seguridad.
11. **Crear un plan de respuesta a la violación de datos** que permita cerrar cualquier vulnerabilidad y limitar el daño que la brecha puede hacer.
12. **Garantizar el cumplimiento normativo** en toda la organización y estar al tanto de los cambios que pudieran producirse en la legislación.
13. **Realizar evaluaciones de las amenazas** y estudiarlas mediante técnicas de análisis que permitan estar mejor protegido.
14. **No usar diccionarios ni algoritmos de descifrado, que se podrían hackear, sino usar reglas de enmascaramiento fijas o aleatorias.**
15. **Sustituir los encriptados por enmascaramiento** o hacer una encriptación centralizada y llevada a cabo por el propio producto.

Seguridad de datos: Protege los datos sensibles de tu organización

Haz click *aquí* y descubre cómo hacerlo a través de este video online.

Responsabilidades en materia de seguridad de datos

> Los encuestados aumentaron sus presupuestos de seguridad de la información en un 67% en 2015.

PricewaterhouseCoopers "Global Information Security Survey 2016

¿Quién es responsable de la integridad y seguridad de los datos? ¿Y si esa información está en la nube? ¿Quién se responsabiliza de cualquier pérdida de datos o violación de seguridad?

El desconocimiento de la ley no exime de su cumplimiento, igual que el no saber dónde residen los datos o de dónde provienen no implica que pueda actuarse de forma poco responsable con ellos. Y, lo cierto es que **todos somos responsables**, desde el primero hasta el último en cada organización.

La seguridad en la nube es una frontera nueva y en evolución, tanto para las empresas, como para los mismos proveedores de la nube. **La comprensión de los roles, las responsabilidades y las obligaciones en materia de seguridad en el cloud es una prioridad** para asegurarse de que los datos están protegidos, así en la nube como en su propio centro de datos.

Recientes estudios revelan que existe una gran confusión al respecto, sobre todo cuando se trata de entornos cloud. En concreto, una investigación de *Ponemon Institute* pone de manifiesto que:

- **El 63% de las personas desconocen qué medidas de seguridad utilizan los proveedores de la nube para proteger los datos confidenciales.**
- **El 44% considera que el principal responsable de la seguridad de los datos es el proveedor de la nube.**

En la práctica, mientras que los propietarios de los datos son, en última instancia, responsables de mantener la seguridad y el control de su información, la nube introduce un **nivel compartido de responsabilidad entre el propietario de los datos y el proveedor de servicios. Pero existen diferencias**, por ejemplo:

1. **En el caso de Saas y PaaS no hay mucho margen para que las empresas desplieguen soluciones de seguridad de datos o de gobernabilidad** en este tipo de entornos, puesto que el proveedor es propietario de la mayor parte de aspectos en relación con la seguridad e IT.
2. **En lo referente a la infraestructura como servicio (IaaS) existe un mayor equilibrio.** La responsabilidad está más repartida y los proveedores proporcionan un nivel básico de seguridad, como pueden ser los firewalls, siendo su cliente el encargado de añadir todos los extras de seguridad que considere necesarios a partir de ahí, para **garantizar la protección de sus datos.**

Cuando nada de esto parece suficiente, existe la opción de recurrir a ciertas ofertas de seguros cibernéticos que protegen contra eventos como la extorsión cibernética, la pérdida de servicio o la violación de la confidencialidad de datos.

Pero, además, **cada organización debe asegurarse de que todos los empleados son conscientes de la necesidad de su involucración en el plan de seguridad de datos corporativo, de su compromiso adquirido como propietarios de los datos y de su responsabilidad como parte de la empresa**. Lamentablemente, la realidad muestra que todavía queda mucho trabajo por hacer a este respecto. Así lo demuestra un reciente estudio de Absolute Software:

- El 52% de los encuestados usan sus dispositivos propiedad del empleador para uso personal.
- El 21% de los encuestados han modificado la configuración predeterminada en sus dispositivos de trabajo.
- **El 14% de todos los encuestados cree que su comportamiento compromete la seguridad de su organización.**

Los datos todavía resultan más preocupantes cuando se refieren a los trabajadores de entre 18 y 34 años, conocidos como *millenials* ya que en su caso son un 64% quienes no tienen reparos en utilizar los dispositivos que les ha proporcionado la empresa para uso personal, reconociendo además que acceden a lugares poco seguros en el 27% de los casos.

Dificultades a la hora de garantizar la seguridad

> El 50% de los empleados cree que la seguridad de los datos no es su responsabilidad.
>
> *Absolute Software*

Una de las **técnicas más aconsejables para mantener los datos protegidos y garantizar su seguridad es el enmascaramiento**. Sin embargo, para la aplicación de esta técnica es importante **confiar en profesionales con experiencia**, capaces de superar dificultades como las siguientes:

- En ocasiones, el campo a enmascarar es una tabla primaria y puede afectar a las demás, a todas las hijas que usan esa clave. **El dominio de la técnica será clave para mantener la integridad de todas las referencias** de ese campo en las hijas.
- Al **plantear una acción de data masking** puede no tenerse en cuenta que la existencia de longitudes de datos inviables. Esto puede suceder en los casos en que la longitud del dato es menor que la del dato enmascarado.
- Otro inconveniente tendría que ver con los casos en que se requiere enmascarar con un número pero se descubre que sólo se puede hacer con un stream.
- Una complicación frecuente tiene que ver con los tipos de datos. Siempre **ha de buscarse un número aleatorio que se parezca al real para evitar problemas a la hora de cruzarlos y que todavía resulten válidos.**
- Pueden presentarse también problemas de llenado de log, que se presentarían al trabajar con volúmenes de datos muy grandes, que hacen que la iniciativa pierda viabilidad al exceder el plazo estimado para el enmascaramiento. **Es preciso adaptarse a la ventana de ejecución disponible.**
- Por último, no hay que olvidarse de las dificultades en relación con las fechas de auditoría o cualquier otro tipo de presión de tiempo para el proyecto. En la práctica, puede suceder que el enmascaramiento de deje para el final, sin reparar en que **este tipo de proyectos necesitan de un tiempo y ese margen no se puede reducir demasiado.**

Cómo llevar a cabo un proyecto de seguridad de datos

Un **proyecto de seguridad de datos** necesita de un plan sólido y la consistencia de éste dependerá de la **capacidad de la organización para hacerse las preguntas adecuadas**. Cuestiones acerca de:

- ¿Quiénes son los responsables de los datos.
- ¿Qué datos son sensibles.
- ¿Cuáles son los diferentes niveles de criticidad en la información corporativa.
- ¿Cuáles son las fuentes de datos.
- ¿Qué medios se emplean para recoger y transmitir datos desde esas fuentes.
- ¿Cómo se puede asegurar el proceso.
- ¿Dónde se almacenan los datos.
- ¿Será necesario ampliar la capacidad de almacenamiento.
- ¿Quién tiene acceso a los datos.
- ¿Los accesos se producen en condiciones de consistencia?
- ¿En qué consiste el plan de recuperación y backup?
- ¿En qué consiste el plan de data archiving?
- ¿Dónde se conservarán estos archivos?

La fuerte postura de seguridad y la **implementación de un plan integral de privacidad y seguridad de datos** es la medida más efectiva que las empresas pueden emplear para mitigar los costos significativos de remediar una violación de datos. Para definir este plan hace falta:

a) Entender qué tipo de información se está recopilando y qué requisitos imponen las leyes, reglamentos y otras políticas de cumplimiento interno.

b) Implementar procedimientos internos para asegurar el cumplimiento de dichas leyes y regulaciones. Especificar qué tipo de medidas se tomarán para proteger los datos en los diferentes entornos, eligiendo las técnicas más adecuadas en cada caso, como puede ser el enmascaramiento de datos.

c) Ocuparse de determinar las políticas de retención y destrucción de datos, las políticas de privacidad, los procedimientos de seguridad de datos, los planes de aviso de violación de datos, los programas de capacitación de empleados, los acuerdos de uso de equipos informáticos y los procesos internos de auditoría y monitorización, al desarrollar el plan de seguridad de datos.

d) Reunir a un equipo de personas de la organización, de las áreas de IT y negocio, que se **responsabilicen de garantizar la seguridad de la información**, el cumplimiento de la privacidad y la protección de datos.

e) Terminar de perfilar el plan, implementarlo **y realizar auditorías regulares para medir su eficacia.**

Beneficios de la seguridad de datos para la organización

Existen numerosas razones para invertir esfuerzo, tiempo y dinero en la protección de datos. Entre los principales **beneficios de garantizar un buen nivel de seguridad de la información** se encuentran:

- **Disminuir el riesgo de pérdidas financieras,** como las que tienen que ver con las multas que se imponen por la pérdida de información, las ventas perdidas o los gastos de las costas procesales, caso de llegar a ese punto.
- **Evitar el deterioro de la imagen corporativa**, que comenzaría por el abandono de clientes y la pérdida de confianza de los inversionistas.
- **Asegurar la protección adecuada de la información valiosa, que aporta tranquilidad, marca distancia con la competencia y permite operar normalmente.**
- **Garantizar el cumplimiento normativo.**
- **Impulsar la productividad,** que se ve reducida cuando los problemas de seguridad impiden a los empleados trabajar normalmente con las bases de datos de clientes o los activos informacionales de la organización; o cuando la pérdida de datos provoca fallos en aplicaciones y sistemas.

Y tu negocio, ¿ya disfruta de estas ventajas? ¿Conoces el enmascaramiento de datos? ¿Sabes dónde y cuándo te interesaría más aplicar esta técnica?

¿Tienes dudas de cómo mejorar la seguridad de los datos de tu empresa?

Haz click *aquí* para agendar una consulta gratuita con uno de nuestros expertos en Seguridad de Datos.

PowerData
Especialistas en Gestión de Datos

ESPAÑA

MADRID

C/ Miguel Yuste, 17, 4º, C
28037 Madrid
Tel:(+34) 91 129 72 97
marketing@powerdata.es
www.powerdata.es

BARCELONA

C/ Pau Claris, 95
08009 Barcelona
Tel: (+34) 934 45 60 01
marketing@powerdata.es
www.powerdata.es

VALENCIA

Edificio Europa - 5º I Avda. Aragón, 30
46021 Valencia
Tel: (+34) 960916025
marketing@powerdata.es
www.powerdata.es

LATINOAMÉRICA

ARGENTINA

Avenida Leandro N Alem 530, Piso 7
CD C100 1AAN Ciudad Autónoma de Buenos Aires
Tel: (+54) 11 5235 7126
marketing@powerdataam.com
www.powerdataam.com

CHILE

Padre Mariano Nº 82 - Oficina 602
Las Condes, Santiago CP 7550357
Tel: (+56) 2 29363-100
marketing@powerdataam.com
www.powerdataam.com

COLOMBIA

Carrera 16 # 93 A - 16 oficina 504 Tel: (+57 1) 6167796
Bogotá
Tel: (+57 1) 6167796
marketing@powerdataam.com
www.powerdataam.com

MÉXICO

Homero 906, Colonia Polanco, Miguel Hidalgo
C.P. 11550, México, D.F.
Tel: +(52) 55 5203 1771
marketing@powerdataam.com
www.powerdataam.com

PERÚ

Calle Los Zorzales Nº 160, piso 9
San Isidro, Lima 27
Tel: (+51) 1 6344900
marketing@powerdataam.com
www.powerdataam.com

Síguenos en: