Normativas e IA impulsan una mejor gestión de la privacidad

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

Con la proliferación de las redes sociales y las estrategias de personalización de las ofertas comerciales, hoy las organizaciones recopilan más que nunca una enorme cantidad de información personal, que van desde el nombre propio, el correo y el número telefónico, hasta fotografías y datos de tarjetas de crédito. Todos los servicios y aplicaciones que requieren registro, solicitan información personal a cambio de alguna oferta para el usuario. Pero con un gran tesoro de datos debería venir también una gran responsabilidad, y como muchas empresas no lo asumían, la legislación entró a rectificar el tema. Presto: Las políticas de privacidad de la información, que hoy son obligatorias.

Aplicada a la protección de datos, la privacidad de la información está relacionada con la capacidad que una organización o individuo tiene para determinar qué datos en sus sistemas pueden ser compartidos con terceros. Por ello, una política de privacidad debe explicar qué datos de

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

identificación personal de sus clientes, proveedores o empleados está recopilando una organización, así como qué se hace con ellos y cómo se manejan. En esta guía esencial no analizaremos esas políticas, sino que daremos un vistazo al panorama de la privacidad de los datos como parte del cumplimiento corporativo, y a su importancia cada vez mayor, especialmente bajo el horizonte del desarrollo de las plataformas de analítica e inteligencia artificial.

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco

Melisa Osores, Managing Editor para América Latina

Las empresas de todo el mundo que realizaron inversiones para mejorar sus prácticas de privacidad de datos han comenzado a recibir beneficios tangibles, dio a conocer el Estudio de referencia de privacidad de datos de Cisco 2019. El informe revela el vínculo entre las buenas prácticas de privacidad y los beneficios comerciales, pues los encuestados informaron sobre menos retrasos en las ventas y la baja en los costos por las violaciones de datos.

“La relevancia de la privacidad y de la protección de los datos aumentó dramáticamente el año pasado. Los datos son la nueva moneda y, a medida que el mercado cambia, vemos que las organizaciones se están dando cuenta de los beneficios reales de sus inversiones en la protección de datos”, declaró la directora de privacidad de Cisco, Michelle Dennedy. "En Cisco, creemos absolutamente en la importancia de proteger a nuestros clientes y en impulsar el éxito del negocio al maximizar el valor de los datos y minimizar el riesgo".

El Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea, que se centra en aumentar la protección de la privacidad y los datos personales de los residentes de la UE, entró en vigor en

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

mayo de 2018 y las organizaciones de todo el mundo han estado trabajando constantemente para cumplir con esta normativa. De acuerdo con el estudio de Cisco, el 59% de las organizaciones informó haber cumplido con todos o la mayoría de los requisitos, el 29% espera hacerlo dentro de un año y 9% tomará más de un año en hacerlo.

El reporte muestra que los clientes están cada vez más preocupados porque los productos y servicios que implementan brinden las protecciones de privacidad adecuadas. Aquellas organizaciones que invirtieron en privacidad de datos para cumplir con el GDPR experimentaron retrasos más cortos debido a preocupaciones de privacidad en la venta a clientes existentes: 3.4 semanas frente a 5.4 semanas para las organizaciones menos preparadas. En general, el retraso promedio en las ventas fue de 3.9 semanas en la venta a clientes existentes, en comparación con las 7.8 semanas reportadas hace un año.

Adicionalmente, las organizaciones preparadas para GDPR mencionaron una menor incidencia de violaciones de datos, menos registros afectados por incidentes de seguridad y menores tiempos de inactividad del sistema. También fueron menos propensas a tener una pérdida financiera significativa debido a una violación de datos.

Más allá de esto, el 75% de los encuestados mencionó que están obteniendo múltiples y amplios beneficios de sus inversiones en privacidad, que incluyen una mayor agilidad e innovación como resultado de contar con controles de

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

datos apropiados, obtener una ventaja competitiva y una mayor eficiencia operativa al tener los datos organizados y catalogados.

“Esta investigación proporciona evidencia de algo que los profesionales de la privacidad han comprendido hace mucho tiempo: que las empresas se están beneficiando de sus inversiones en la privacidad, más allá del cumplimiento. El estudio de Cisco demuestra que un fuerte cumplimiento de la privacidad acorta el ciclo de ventas y aumenta la confianza del cliente", señala Peter Lefkowitz, director de Riesgos Digitales de Citrix Systems y presidente de la Junta Directiva (2018) de la Asociación Internacional de Profesionales de la Privacidad (IAPP).

Otros hallazgos clave del reporte, que se basó en una encuesta realizada a más de 3.200 profesionales de seguridad y privacidad de 18 países, incluyen:

- El 87% de las empresas experimentan retrasos en su ciclo de ventas debido a las preocupaciones de privacidad de los clientes o prospectos, en comparación con el 66% del año pasado. Esto se debe probablemente a la mayor conciencia sobre la privacidad provocada por GDPR y las frecuentes violaciones de datos en las noticias.
- Los retrasos en las ventas por país variaron de 2.2 a 5.5 semanas, con Italia, Turquía y Rusia en el extremo inferior del rango, y España, Brasil y Canadá en el extremo superior. Las mayores demoras en las ventas pueden atribuirse a áreas donde los requisitos de privacidad son altos o en transición. Las ventas retrasadas pueden causar un déficit de ingresos relacionado con la compensación, la financiación y las relaciones con los inversores. Las ventas retrasadas también pueden

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

convertirse en ventas perdidas, si un cliente potencial compra a un competidor o decide no comprar en absoluto.

- Las principales razones citadas para los retrasos en las ventas incluyen investigar las solicitudes de los clientes con relación a las necesidades de privacidad, traducir la información de privacidad a los idiomas de los clientes, educar a los clientes sobre las prácticas de privacidad de una organización, o rediseñar los productos para satisfacer las necesidades de privacidad de los clientes.
- Por país, la capacidad para estar preparados para el GDPR varió de 42% a 75%. España, Italia, Reino Unido y Francia estaban en la parte superior del rango, mientras que China, Japón y Australia estaban en el extremo inferior.
- Solo 37% de las compañías preparadas para GDPR experimentaron una violación de datos que costó más de 500 mil dólares en comparación con el 64% de las empresas menos preparadas para GDPR.

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

Brasil se prepara para lanzar ley de protección de datos personales

Vincent Quezada, CEO

El año 2018 pasará a la historia como aquél en que la privacidad se ha convertido en un factor de suma importancia, tanto para los individuos, las empresas y los gobiernos.

En Brasil, el Senado aprobó, el pasado martes 10 de Julio de 2018, el Proyecto de Ley de la Cámara (PLC) 53/2018 que, en caso de obtener la sanción presidencial, significaría que la nación sudamericana pasaría a formar parte de los países que cuentan con una legislación específica para la protección de datos y la privacidad de sus ciudadanos.

El texto disciplina la forma en que las informaciones se recogen y tratan, especialmente en medios digitales, como datos personales de registro o incluso textos y fotografías publicadas en redes sociales.

¿Por qué es tan importante? Si entra en vigor, la llamada Ley General de Protección de Datos Personales establecerá una serie de reglas que empresas y otras organizaciones actuantes en Brasil tendrán que seguir para permitir que

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

el ciudadano tenga más control sobre el tratamiento que se le da a su información personal.

El proyecto es un paso necesario y relevante. Actualmente, la legislación brasileña es muy vaga en cuestiones relacionadas con datos personales y privacidad. Existen leyes que garantizan el derecho a la intimidad y al secreto de comunicaciones, por ejemplo, pero se establecieron en circunstancias que no contemplaban el escenario tecnológico actual.

La consecuencia de esto es que muchas empresas, particularmente los proveedores y operadores de telecomunicaciones, acaban no dando la debida importancia al asunto. Cuando se les pregunta, estas organizaciones a menudo hacen interpretaciones evasivas al respecto o simplemente dicen que no hay obligación legal de seguir protocolos completos para la protección de datos. También puede haber negligencia en el tratamiento de datos personales en las esferas gubernamentales.

¿Qué es exactamente la Ley General de Protección de Datos Personales?

El nombre es autoexplicativo: Se trata de una legislación que determina cómo los datos de ciudadanos pueden ser recogidos y tratados, y que prevé castigos para transgresiones. El propio Senado reconoce que la propuesta para el marco general de protección de datos (otra denominación dada a la propuesta)

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

estuvo fuertemente inspirada en el GDPR, un riguroso conjunto de reglas sobre privacidad de la Unión Europea que entró en vigor en mayo.

La búsqueda de una legislación que regule el tratamiento de datos no es nueva. El Proyecto de Ley de Cámara (PLC) 53/2018 tiene como base al menos otras dos propuestas que tramitan en la Cámara de Diputados (PL 4060/2012 y PL 5276/2016), además de un Proyecto de Ley del Senado (PLS 330/2013).

La unión de estos proyectos, y algunas revisiones, hacen que la Ley General de Protección de Datos Personales, de la forma en que fue aprobada por el Senado, contenga diez capítulos con 65 artículos que determinan cómo pueden ser recogidos y tratados los datos personales en Brasil, especialmente en lo que se refiere a los derechos en los medios digitales.

El proyecto trata como dato personal cualquier información relacionada a una persona que, aisladamente o en conjunto con otros detalles, permite identificarla. Algunos ejemplos de datos son: nombre, apodo, dirección residencial, dirección de correo electrónico, dirección IP, fotos propias, formularios de registro y números de documento.

¿Cómo deben tratarse y colectarse los datos personales? Para empezar, las organizaciones públicas y privadas solo podrán recopilar datos personales si tienen el consentimiento del titular. La solicitud deberá ser hecha de manera clara para que el ciudadano sepa exactamente lo que va a ser recolectado,

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

para qué fines serán usados y si serán compartidos. Cuando haya implicación de menores de edad, los datos solo podrán ser tratados con el consentimiento de los padres o responsables legales.

Si hay cambios de propósito o traspaso de datos a terceros, un nuevo consentimiento deberá ser solicitado. El usuario podrá, cuando desee, revocar su autorización, así como solicitar acceso, exclusión, portabilidad, complementación o corrección de los datos. En caso de que el uso de la información lleve a una decisión automatizada indeseada, por ejemplo, el rechazo de financiamiento por parte de un banco, el usuario podrá solicitar una revisión humana del procedimiento.

Hay una categoría clasificada como "datos sensibles". Ella se refiere a informaciones como creencias religiosas, posicionamientos políticos, características físicas, condiciones de salud y vida sexual. El uso de estos datos será más restrictivo. Ninguna organización podrá hacer uso de ellos para fines discriminatorios. También será necesario asegurarse de que se protejan adecuadamente.

En general, la idea es proteger al ciudadano del uso abusivo e indiscriminado de sus datos. Además de pedir consentimiento de manera clara y atender a las demandas del usuario sobre el mantenimiento o eliminación de los datos, las organizaciones solo podrán solicitar los datos que realmente son necesarios al final propuesto. En ese sentido, el usuario podrá cuestionar si la exigencia de determinado dato tiene sentido o utilidad.

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

Hay excepciones. Las reglas no valen para datos personales tratados con fines académicos, artísticos o periodísticos, así como para aquellos que involucra seguridad pública, defensa nacional, protección de la vida y políticas gubernamentales. Estos casos deben ser tratados por leyes específicas.

Qué sucede en caso de pérdida de datos

Las fugas o problemas de seguridad que comprometen datos personales deberán ser informados a las autoridades competentes a su debido tiempo. Tras el análisis de la situación, las autoridades indicarán los próximos pasos, como determinar que el problema se divulgue a la prensa.

El castigo por incumplir la ley depende de la gravedad de la situación. Si se comprueba la infracción, la empresa u organización responsable podrá recibir desde advertencias hasta una multa equivalente al 2% de su facturación, pero limitada al valor máximo de R$ 50 millones de reales.

La empresa u organización también podrá tener las actividades ligadas al tratamiento de datos total o parcialmente suspendidas, además de responder judicialmente a otras violaciones previstas por ley, cuando sea el caso.

¿Aplica solo para las empresas brasileñas? El origen de la empresa u organización no es un factor de excepción. La propuesta vale para operaciones de tratamiento de datos realizadas en Brasil o en otro país, siempre que la

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

recolección de datos sea hecha en territorio brasileño. Esto significa que, si por ejemplo, Google recoge datos de un usuario dentro de Brasil, pero los procesa en los Estados Unidos, tendrá que seguir la legislación brasileña.

En caso necesario, la empresa podrá transferir los datos a una filial o una sede extranjera, a condición de que el país de destino también tenga leyes exhaustivas de protección de datos o pueda garantizar mecanismos de tratamiento equivalentes a los que se exigen en Brasil.

En caso de que los datos ya no sean necesarios –cuando una cuenta o servicio haya finalizado, por ejemplo– la organización tendrá que borrarlos, a menos que haya obligación legal u otra razón justificable para su preservación

Para vigilar y sancionar la aplicación de la ley, el proyecto prevé la creación de la Autoridad Nacional de Protección de Datos (ANPD), autarquía ligada al Ministerio de Justicia, que deberá fiscalizar y garantizar la aplicación de la ley. También está prevista la creación del Consejo Nacional de Protección de Datos Personales y de la Privacidad, que estará formado por 23 representantes del poder público y de la sociedad civil. El grupo realizará estudios, debates y compañeras referentes al asunto.

Tanto la iniciativa privada como los organismos públicos tendrán que indicar a un responsable del tratamiento de datos dentro de la organización. Las eventuales solicitudes o comunicaciones referentes a datos personales serán tratados prioritariamente con esa persona.

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

Para entrar en vigor, el proyecto de la Ley General de Protección de Datos Personales necesita primero pasar por la sanción del presidente de Brasil, Michel Temer. Después de ese procedimiento, habrá un plazo de 18 meses para que sectores privados y públicos se adecúen a la ley.

A menos que la propuesta sea vetada, revisada o tenga el plazo ampliado por algún motivo (lo que no es inusual en Brasil), es de esperar que la ley entre en vigor a comienzos de 2020.

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores

Niel Nickolaisen, CTO

Hice una presentación hace unos días en una de nuestras universidades locales. Mi tema era el mundo que pronto será, en el que cada trabajo es un trabajo de TI. Mi punto era que ahora tenemos que ajustar nuestro enfoque de la educación y la formación y preparación de carrera para que cada uno desarrolle las habilidades que necesita tener (y que nosotros necesitamos que tengan), porque pronto cada actividad utilizará la tecnología. Como ejemplos, hablé de cómo la medicina y los tratamientos cambian cuando todos llevamos biosensores que informan nuestras estadísticas vitales a alguien, y cómo el trabajo de un fontanero será diferente cuando las válvulas y las tuberías informen de su salud y, en un futuro no muy lejano, hagan un cierto nivel de autosanación.

Cubrí las mega-tendencias que nos están conduciendo hacia un lugar de trabajo donde "todos los trabajos son trabajos de TI". Mencioné la internet de las cosas (IoT), que es impulsada por cómputo más pequeño, más inteligente y

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

más barato (es decir, microprocesadores en todo), con comunicación disponible a través de banda ancha ubicua, por cable e inalámbrica.

Expliqué que, en paralelo, seguimos avanzando en los sistemas cognitivos, los cuales, cuando se combinan con cómputo más pequeño, más inteligente y más barato, crean un futuro de lo que llamo "nanotecnología pensante". Por cierto, en mi tiempo libre, a veces me gustaría haber nacido 20 años antes, para no tener que tratar o pensar acerca de todo esto; mi papel de líder de TI ya es lo suficientemente difícil antes de llegar a la tecnología en todas partes y en todo.

Es posible que se esté preguntando: "¿Por qué está Niel hablando de todo esto cuando nuestro tema de este mes es la seguridad y privacidad de datos de la IoT?". Para mi mente febril de CTO, esto importa porque a medida que aplicamos sensores inteligentes a todo, y esos sensores informan sobre todo, tenemos que clasificar no solo lo que podemos y debemos hacer con esos datos, sino también quién posee esos datos.

La seguridad y privacidad de los datos de la IoT en el lugar de trabajo

Veamos un ejemplo actual. Supongamos que, como parte de una iniciativa de bienestar organizacional, mi empleador me da un vestible de salud para que pueda realizar un seguimiento de mis pasos y mi sueño y mi ritmo cardíaco, y cualquier dato que el vestible pudiera recoger. ¿Quién posee esos datos?

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

¿Quién tiene acceso a esos datos? Supongamos que llamo para decir que estoy enfermo un día, pero mi vestible me muestra tomando unos mil pasos –con el consiguiente aumento de la frecuencia cardiaca– porque decidí no ir al trabajo e ir a una caminata de montaña o a caminar en la playa. ¿Debe mi empleador saber eso? ¿Debe mi empleador saber que –según lo informado por el vestible provisto– soy un vago que rara vez se mueve de mi sillón reclinable? ¿Qué pasa si mi empleador decide que los vagos como yo deben pagar más por el seguro médico que las personas deportistas entre nuestras filas? Ahora, extrapole estos ejemplos a un futuro cercano con más sensores, que capturan más datos personales e informan esos datos a alguien. ¿Quién es el propietario de los datos y quién tiene acceso a los datos?

Estoy seguro de que hay gente con grandes cerebros y fuertes opiniones que van a resolver la seguridad y privacidad de los datos de la IoT –al menos espero que lo hagan– ¿pero qué podemos hacer mientras tanto?

Vamos a empezar con una regla básica de oro. Es decir, no importa lo que suceda con las regulaciones y la política, nuestra regla de oro debe ser que una persona controla lo que sucede con cualquier dato sobre ella. Eso significa que una persona puede elegir o no que sus datos sean compartidos (esto ya es la base de las leyes de privacidad de la Unión Europea).

A medida que diseñamos y desarrollamos nuestros sistemas, vamos a anticipar que los datos de una persona le pertenecen a ella. También vamos a anticipar que nuestros procesos, políticas y prácticas deben mantener los datos

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

individuales privados y seguros. En la práctica, esto significa que tenemos que cumplir con algún marco como ISO 27001 o SSAE 16, por lo que sabemos que tenemos juntos nuestros actos de seguridad de la información y privacidad, incluyendo la seguridad y privacidad de datos de la IoT.

Si anticipamos que nuestros clientes (y potencialmente empleados) pueden optar por decir que sí o que no utilicemos sus datos, eso ejerce presión sobre el diseño de nuestros sistemas para asegurar que nuestra funcionalidad es tan convincente que nuestros clientes nos permitirán utilizar sus datos en nuestros sistemas. Debemos esperar que nuestra organización querrá reunir y utilizar datos de individuos (de lo contrario, ¿por qué tratar con los dolores asociados con tenerlos?), y por lo tanto, también esperar garantizar que nuestro uso de esos datos beneficia a nuestros clientes con tanta fuerza que optarán por aceptar que tengamos y usemos sus datos.

En nuestra empresa, estamos empezando a utilizar los datos individuales para dar a nuestros clientes una visión que les ayude a alimentar y desarrollar a sus empleados, de una manera única y convincente. Si podemos entregar eso, espero que la mayoría esté dispuesta a dejarme consumir sus datos. No tengo ninguna duda de que los datos individuales que recogemos pronto incluirán datos de la IoT.

Las empresas necesitarán toda la experiencia que puedan para obtener beneficios de ello y garantizar la seguridad y privacidad de los datos de la IoT.

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

Al terminar mi presentación en la universidad, sugerí que la escuela revise su plan de estudios a fin de que todas las carreras incluyan una especialidad de TI o al menos un núcleo de cursos de TI. No estoy seguro en cuanto a la probabilidad de un cambio tal, pero sí creo que eso lo que nuestro nuevo mundo necesita.

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

Utilice los “vestigios digitales” sin afectar la privacidad

Sin importar el tipo de página que visitemos, al navegar por internet dejamos "vestigios digitales”; es decir, esparcimos "rastros" de nuestra actividad, incluso cuando conducimos nuestro coche usando aplicaciones GPS. Las empresas, los gobiernos y otras organizaciones recopilan esta información, pero, ¿con qué fin? De acuerdo con Unify, hay cinco principales tipos de uso para estos datos.

Primero, el uso de datos de segundos o terceros que se usan en planes de marketing y estrategias corporativas; segundo, las empresas usan los datos de los usuarios para evaluar a los participantes de la conversación; tercero, los datos capturados con el uso de sensores inteligentes que trabajan dentro de la lógica de la "internet de las cosas" (IoT); cuarto, la información personal que se usa como “moneda"; quinto, lo que se conoce como el factor de "privacidad inquietante".

Cercando toda esta colección y procesamiento de datos está el hecho de que esto no sería posible sin el crecimiento exponencial de la capacidad computacional en las últimas décadas. En este sentido, el uso de datos de terceros será cada vez más común en nuestra rutina, y se convertirán en un referente para las empresas para deducir el por qué de algunas acciones humanas, es decir, como puntos de información con el fin de mejorar y perfeccionar sus productos.

Un buen ejemplo de esto puede ser una tableta que permite la lectura de libros electrónicos, y puede recoger datos de interés para los autores del libro, como

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

la velocidad media de pasar las páginas o los puntos de parada en la lectura de una obra. Conceptualmente, los escritores podrían utilizar estos datos para saber dónde sus libros ganan o pierden impulso de lectura, para ajustar sus estilos de escritura.

Así, los datos reflejan la manera cómo actúan los individuos, y las organizaciones pueden utilizar estos elementos para crear nuevos modelos de negocio. Esta gran oportunidad solo existe debido a la enorme cantidad de datos que ahora se agregan a las nubes, y a la gran habilidad para computar estos datos. Desarrollando las matrices y los algoritmos correctos, las empresas pueden ganar la capacidad de conocer incluso el rendimiento de sus empleados, consultores o cualquiera de los implicados en sus negocios.

Pero, ante este panorama con más y más datos (clics, localizaciones, llamadas telefónicas, mensajes de texto, aplicaciones, etc.) siendo recogidos, es lógico preguntarse: ¿en qué punto nuestra información personal se convierte en un tipo de "moneda" con sus propias reglas y derechos?

Al respecto, lo único cierto en relación con el factor de la "privacidad inquietante" es que los individuos regulan de manera parcial sus filtros: por una parte, el consumidor está dispuesto a renunciar a una gama de información a cambio de beneficios como el uso de sitios sin cargos. Por otra parte, los consumidores hacen esta misma información disponible a condición de que no se utilice sin permiso; de lo contrario, consideraría la práctica reprobable.

Por ello, se debe entender los límites cuando se trata del uso de los datos de terceros para crear nuevos modelos de negocio o evaluación de rendimiento. Se debe discutir cómo los consumidores y las empresas negocian las condiciones de un contrato que caben en una lógica de comercio electrónico,

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

cuando se trata de información personal utilizada para promocionar productos a cambio de recuperación financiera.

Los vestigios digitales están en todas partes y, por tanto, es importante evaluar cómo utilizarlos de la mejor manera y cómo los procesos empresariales nutren al factor de "privacidad inquietante".

En esta e-guide

- Invertir en privacidad de datos puede traer beneficios de negocios, dice Cisco
- Brasil se prepara para lanzar ley de protección de datos personales
- La seguridad y privacidad de datos de IoT empieza ahora por los CIO y los educadores
- Utilice los “vestigios digitales” sin afectar la privacidad

Obtener más contenido exclusivo de PRO+

Como miembro de PRO+, tienes acceso a todo el portafolio de más de 140 sitios web de TechTarget. El acceso a PRO+ te dirige a "contenidos exclusivos para miembros platino" que están garantizados para ahorrarte tiempo y esfuerzo de tener que rastrear dicho contenido premium por tu cuenta, ayudándote en última instancia a resolver tus desafíos más difíciles de TI de manera más efectiva y rápida que nunca.

Aprovecha tu membresía al máximo visitando: searchdatacenter.techtarget.com/es/eproducts

Images; stock.adobe.com