PowerData

La integridad de los datos, un punto crítico en la gestión de la información

Te presentamos la guía definitiva para dominar la integridad de datos.

Índice

Qué se entiende por integridad de los datos

La integridad de un dato alude a ese atributo o cualidad que es inherente a la información cuando se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de los datos que la conforman.

Esta cualidad, que va ligada al propio dato y no al lugar donde se almacena, al contrario de lo que sostienen creencias bastante extendidas; se obtiene cuando se impide eficazmente que el contenido de una base de datos, de un proceso o de un sistema se vea, accidental o intencionalmente:

- Modificado, en base a su propio contenido o con ayuda de la inserción de uno nuevo.

- Destruido total o parcialmente.

En Powerdata empleamos herramientas enfocadas a validar los atributos del dato, especialmente en lo que concierne a su calidad, abordando cada uno como un todo, es decir, como un dato exacto, completo y homogéneo.

La importancia de la integridad de los datos

La integridad de los datos tiene un carácter decisivo en cualquier organización; el sector a que se dediquen e incluso su tamaño son indiferentes a la hora de considerar este asunto, y ello se puede ilustrar con sencillos ejemplos que representan situaciones comunes:

- Administración de medicamentos en un hospital: cualquier modificación en los registros electrónicos del tratamiento de un paciente podría tener gravísimas consecuencias para su salud si, por ejemplo, se multiplica o reduce la dosis, al cambiar alguna de las cifras de la dosis diaria que éste necesita de un determinado medicamento.

- Gestión de incentivos desde el Departamento de Recursos Humanos: modificar o eliminar datos dentro de la información de nóminas puede conllevar a un impago o a practicar un cómputo inexacto que no coincida con las condiciones negociadas con el trabajador.

- Elaboración de un reporte gerencial: si se carece de la integridad necesaria entre sistemas, esta falta de integridad afectará a sus relaciones, en primer lugar, lo que provocará que el reporting no pueda beneficiarse de la inteligencia de negocio y no sea, en ningún caso, fidedigno ni válido; situación que podría materializarse en la existencia de fallos al cruzar el total de las ventas con el stock en almacén.

Lo fundamental es, pues, no solo garantizar la integridad de los datos, sino tener la capacidad de descubrir si algo falla, pudiendo detectar anomalías a tiempo. De eso nos ocupamos en Powerdata, cuando validamos los atributos de calidad para posicionar el nivel donde se encuentra cada empresa en cuanto a la calidad del dato, asegurando ese margen de reacción que en tantas ocasiones resulta decisivo.

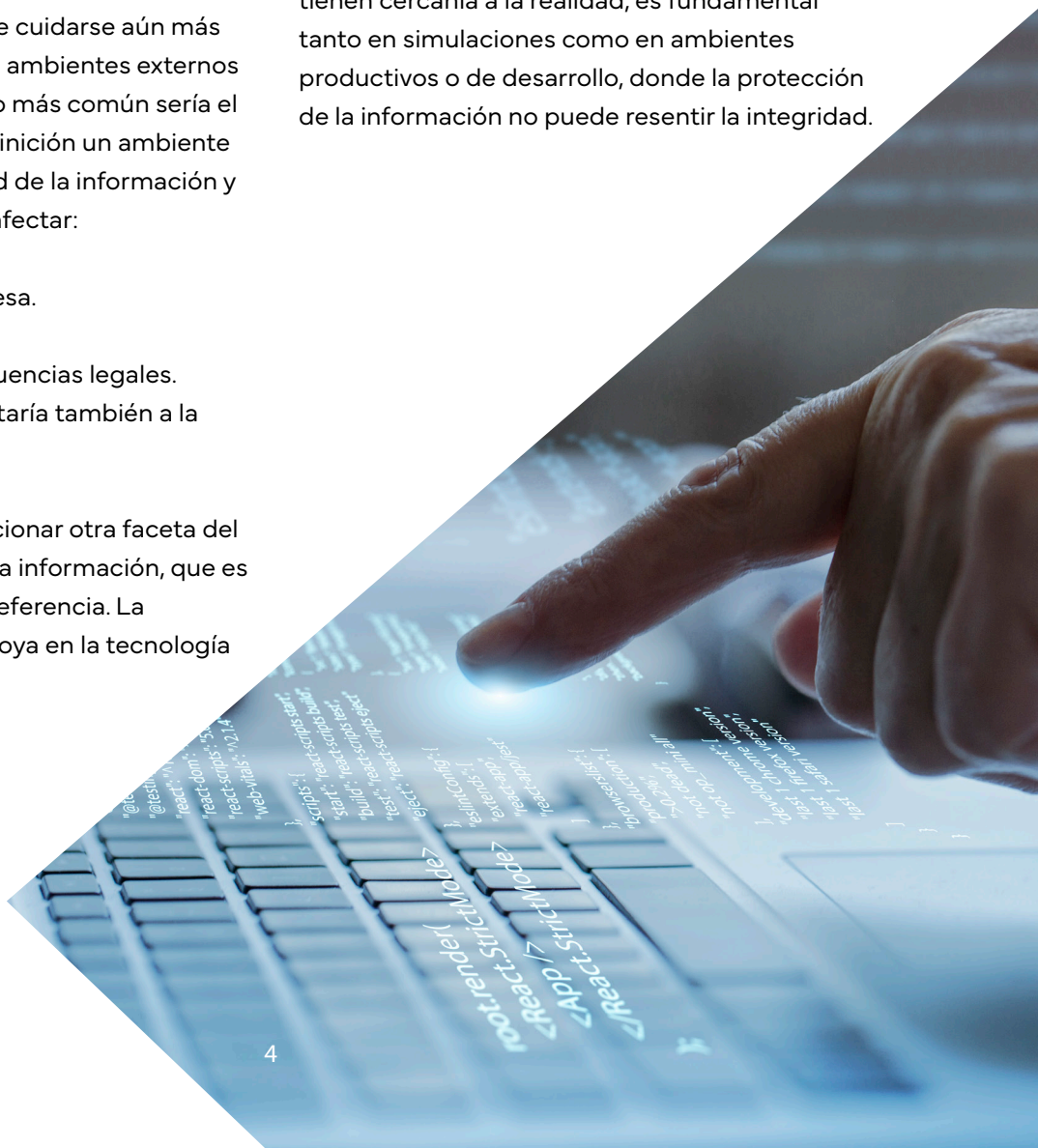
Seguridad de los datos, de la protección a la integridad referencial

Además, a la hora de hablar de la importancia de la integridad de los datos, no puede pasarse por alto que este atributo de la información es uno de los componentes fundamentales de su seguridad. La protección ha de ser exquisita, especialmente cuando escalamos en nivel de criticidad y también cuando hablamos de datos que se exportan a ambientes externos a la empresa. Este aspecto debe cuidarse aún más cuando el dato se exporta a ambientes externos a la organización. El ejemplo más común sería el outsourcing, que es por definición un ambiente vulnerable para la seguridad de la información y que, si se descuida, puede afectar:

- A la imagen de la empresa.
- Al volumen de negocio.
- Podría acarrear consecuencias legales.
- En último término, afectaría también a la gestión interna.

No podemos dejar de mencionar otra faceta del concepto de seguridad de la información, que es la que tiene que ver con la referencia. La integridad referencial se apoya en la tecnología necesaria para proteger la información sensible, aplicando procesos de enmascarado, por ejemplo, en los que, además de cambiar el valor real de los datos, es necesario mantener esa integridad entre ellos.

Procurar que, el enmascaramiento de datos haga posible que éstos puedan utilizarse sin que sean realistas, convirtiéndolos en un conjunto de datos completamente íntegros pero que no tienen cercanía a la realidad, es fundamental tanto en simulaciones como en ambientes productivos o de desarrollo, donde la protección de la información no puede resentir la integridad.



Diferentes visiones en la empresa acerca de la integridad

La integridad de los datos es una de las preocupaciones más importantes en cualquier negocio, sin embargo, dependiendo del sujeto, de sus roles, competencias, responsabilidades, especialización y, por supuesto, de su relación con el dato; existen distintas visiones que completan una perspectiva global sobre esta cualidad de la información.

Visiones de la integridad desde dentro del área de IT o las áreas informáticas:

Esta es la visión más próxima al dato en sí. La cercanía al tratamiento de la información y el grado de expertise de quienes ejecutan las responsabilidades que su puesto determina tiene su principal exponente en tres figuras que se describen a continuación:

- **Security chief:** la visión que este profesional tiene sobre la integridad de los datos se resume en su preocupación por evitar filtraciones de los sistemas a su cargo. Su visión es global y su misión consiste en proteger todos los sistemas de la empresa, imposibilitando que la interacción de terceros con los datos conlleve a su anónima modificación o destrucción.

- **DBA (Data Base Administrator):** a diferencia del jefe de seguridad, esta figura se encarga solamente de la integridad de los datos relacionados con las bases. Su función tiene que ver con que el dato sea insertado correctamente y por eso, concentrará sus esfuerzos en garantizar que los datos que se ingresen no generen problemas. El DBA puede ser una persona o un departamento entero, en función del tamaño y las necesidades de la organización, pero su misión siempre será procurar la coherencia, validez y precisión de la información introducida en las bases de datos.

- **Arquitecto de datos:** mientras que el DBA se preocupa del dato en sí, el arquitecto se ocupa de su estructura y del modo en que ésta se integrará en el sistema. Una de sus funciones es consolidar un modelo que facilite sus relaciones, presentes o futuras con otros sistemas y por eso, al perseguir la integridad, diseña la estructura de las tablas de algún tipo de sistema específico manteniendo entidades primarias únicas, entre otros cometidos. Su trabajo es un factor muy importante cuando se habla de integridad, porque tiene que lograr relacionar cada atributo tanto de manera interna, como de forma externa, plasmándolo en un modelo que resista al paso del tiempo y permita a la empresa evolucionar de acuerdo a sus necesidades.

Integridad de datos: visiones fuera del entorno puramente informático

Al salir del área de IT entramos en un nivel superior, más alejado del dato. Aquí, más que trabajar el dato, se trabaja con él; y, en este ámbito, existen dos figuras que definen perfectamente lo que supone esta perspectiva de la integridad:

- Los encargados de la información: en todas las organizaciones resulta difícil definir esta figura. Se trata de una posición más estratégica y menos operativa. Este profesional es el experto en la materia y precisamente en ello reside la dificultad, ya que muy pocas veces este rol se concentra en una sola persona. Además, al contrario de lo que sucede en el área de IT, donde siempre están definidos los roles, fuera de allí se torna complicado designar a un responsable. Lo que termina sucediendo es que las figuras del área informática mencionadas anteriormente son las que tienen que ejercer de encargadas del dato. Un error que desvirtúa la importancia de su misión, que es fundamental, porque consiste en detectar cuándo un dato no es íntegro, o lo que es lo mismo, cuándo presenta una mala calidad por errores o inconsistencias. El papel de los encargados de la información es definitivamente muy importante en cuanto a las reglas de negocio, y su correspondiente efecto sobre las relaciones entre entidades.
- La propia organización, como propietaria última de la información: para ella, la integridad de los datos supondría el garantizar la existencia de una visión única, basada en el control y en la información de calidad. Esta visión única, integrada y actualizada de los datos asociados a sus entidades clave de negocio, se basaría en la información de calidad y en el seguimiento, tanto de la generación de datos, como de su representación, aludiendo a las responsabilidades de los encargados de la información.

Razones por las que se pierde la integridad de los datos

Los datos se presuponen consistentes, fiables y completos, pero puede suceder que, durante su ciclo de vida, algo les afecte, ya sea de forma voluntaria o involuntaria, y provoque consecuencias para la calidad del dato, para la business intelligence o para la seguridad.

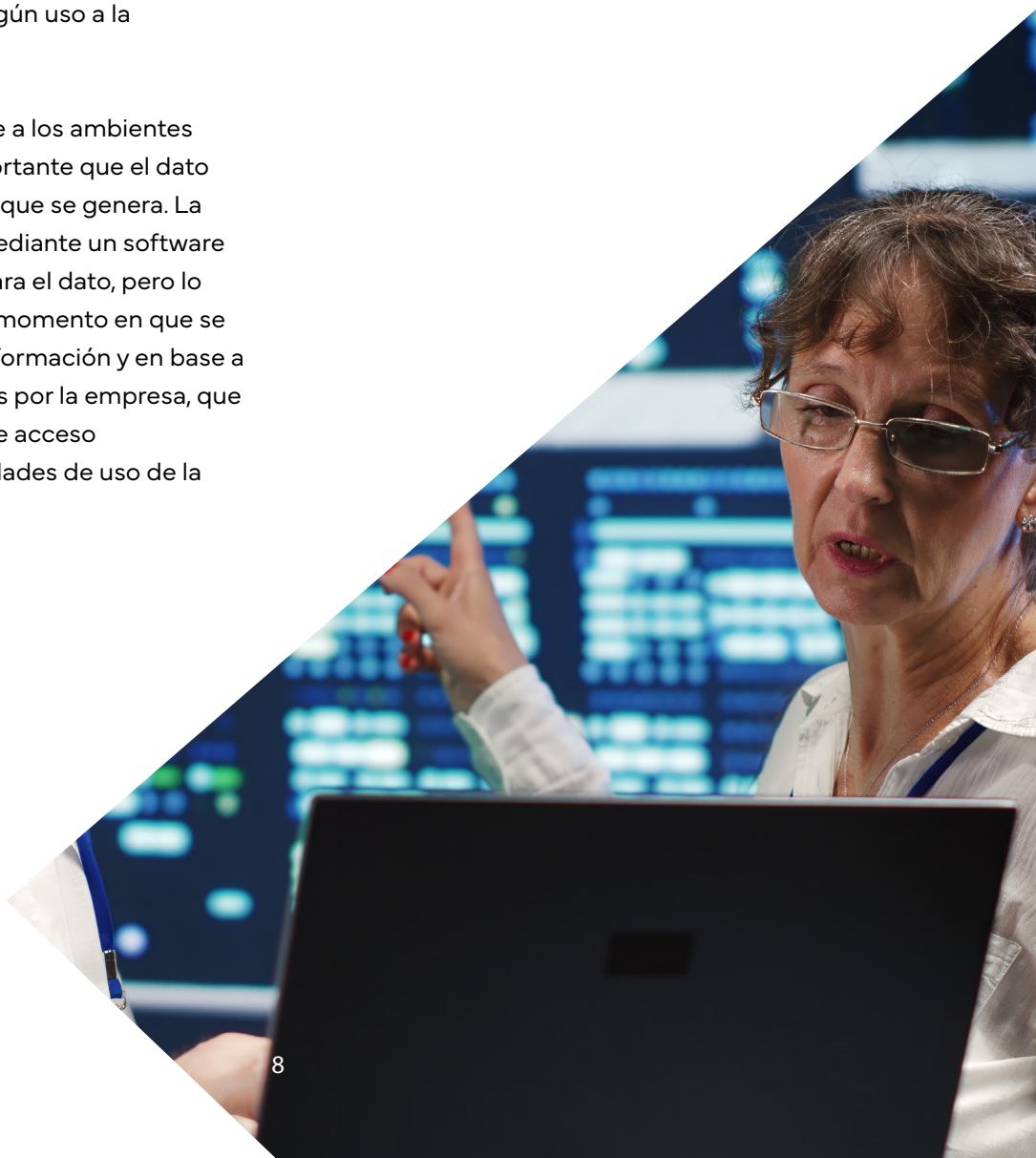
Las causas principales de la pérdida de integridad en los datos

Los principales responsables de la pérdida de integridad de los datos son tres: los datos no estructurados, la introducción manual de datos y los ataques directos a los datos o su modificación intencional.

- Los datos no estructurados: en las empresas es habitual trabajar con formatos como las hojas de cálculo, que son formatos no estructurados y permiten almacenar la información sin ningún control. Este modo de operar afecta directamente a la calidad de los datos, haciendo que la información pierda confiabilidad. El problema se comienza a percibir en la toma de decisiones estratégicas o ejecutivas, basadas en esa información y revestidas de vulnerabilidad.
- La introducción manual de datos: cuando se está trabajando con sistemas, que se presuponen seguros y fiables, la única forma de alterar esta confiabilidad es el error humano. La ausencia de validación de los valores insertados aumenta el riesgo de ingresar los datos erróneamente. Es un hecho: la introducción directa en el sistema puede generar problemas que afecten a los reportes finales, por ejemplo, si quieren hacer proyecciones (de venta, de compra, etc.). Cuando los datos no están bien ingresados, o si están ingresados de manera errónea, el reporte que se genere en función de esa información va a ser totalmente incorrecto. Por eso, la calidad del dato y su integridad son fundamentales cuando hablamos de BI.
- Ataques a la integridad de los datos: tanto estos asaltos como la modificación intencional de los datos afectan obviamente a la seguridad de la información. En este caso, ya no se habla de error humano, sino de la capacidad de modificar el dato, en cualquier fase de su ciclo de vida, en su propia concepción y sin ningún tipo de autorización. Estas fugas o estos cambios provienen en un 80% de dentro de la organización y son mucho más habituales que los ataques causados por agentes que provienen del exterior de la organización.

Powerdata refuerza la seguridad mediante la prevención, gracias a la técnica del enmascarado. Es cierto que existen diferentes tipos de software de seguridad que impiden o tratan de impedir el acceso a los sistemas, pero ¿qué sucede si el protagonista del ataque consigue saltarse todos los controles de seguridad? Es en estos casos donde el enmascaramiento demuestra su efectividad, ya que, si se diese el caso planteado, el agente causante no podría dar ningún uso a la información obtenida.

Esta protección se extiende a los ambientes productivos donde es importante que el dato permanezca intacto desde que se genera. La forma de conseguirlo es mediante un software intermediario que enmascara el dato, pero lo hace exclusivamente en el momento en que se produce la captura de la información y en base a roles previamente definidos por la empresa, que puede establecer niveles de acceso adecuándolos a las necesidades de uso de la información.



Alineamiento con las normas y mejores prácticas

El ámbito de desarrollo de la integridad de los datos queda definido por la normativa vigente en cada país y por las mejores prácticas que las organizaciones decidan incorporar a sus estándares. En este marco evoluciona la concepción que se tiene de la información y de su uso, impulsando siempre a las empresas un paso más allá, en el camino de la mejora continua que se alcanza a través del concepto de calidad total.

Integridad de datos: un buen punto de partida

El alineamiento con las mejores prácticas: la administración y el gobierno de los datos es una de las formas más adecuadas de comenzar a procurar la integridad de los datos.

El Gobierno de los datos: tiene que ver con la concepción de la información y su fuente de origen, la forma cómo la cargo a mi sistema, los diferentes sistemas que recorre el dato hasta llegar a decisiones estratégicas. La información se termina convirtiendo en el imperativo de cada negocio, y es entonces cuando hablamos de gobierno de datos, de tener perspectiva sobre el ciclo de vida del dato. Por eso, Data Governance es decisivo en cuanto a integridad, porque si el dato llega desvirtuado de origen, si se interviene o queda afectado durante su camino, podría cambiar la visión que tengo sobre el negocio.

La administración de datos: alude a referencias más puntuales e implica gestionar de manera correcta cada sistema por separado. Cada lugar donde la información va quedando almacenada necesita contar con un control independiente, que además tiene que estar totalmente centralizado en un gobierno de datos. Así se optimizan los procesos, administrando de forma local, pero manteniendo el control de manera central.

El marco normativo de la integridad de datos

A la vez que evoluciona la tecnología, lo hace también la legislación y con ella la jurisprudencia. Las principales características de esta perspectiva que tanto afecta a las empresas y a la integridad de los datos son:

- Su evolución es irregular y depende de cada país.
- Siempre se produce como una reacción a los avances tecnológicos y, por tanto, siempre se sitúa un paso por detrás de los mismos.
- Es necesario adecuarse a ella por el bien de la empresa, de los trabajadores, de los clientes, de la sociedad, del futuro, etc.

La integridad de los datos deja, mediante esta intervención, de ser una opción para convertirse en una responsabilidad, obligación que impone protección de la información, especialmente de la de carácter sensible; y exige garantías en lo concerniente a la completitud, precisión, confiabilidad, conformidad y consistencia del dato.

Cómo garantizar una mayor integridad en los datos

La integridad de los datos no es un asunto aislado y no se puede gestionar como un ente independiente. Por eso, la incorporación de mejores prácticas, adecuadas a las exigencias legales del entorno de la organización, debe complementarse con la distribución de responsabilidades. La integridad de los datos, responsabilidad conjunta de IT y los procesos de negocios, es en quienes recae la responsabilidad de velar por la integridad de los datos. Su cometido no se reduce a soportar los planteamientos establecidos que les conduzcan, y conduzcan a toda la organización, al fin que se persigue, sino que también se espera de ellos el contribuir a mejorar la seguridad de los datos.

Como se comentaba en el capítulo anterior, la definición y establecimiento de buenas prácticas es un punto de partida idóneo. Y algunos ejemplos de ellas serían:

- Tomar posesión de los datos y asumir la responsabilidad de garantizar su integridad: asimilando la propiedad y responsabilidad de los datos en un mismo sujeto, para potenciar la eficacia de su desempeño.

- Controlar los derechos y privilegios de acceso: estableciendo niveles de interacción que, bien delimitados, definan roles y usuarios en su relación con los sistemas y procesos, o lo que es lo mismo, en su interacción con el dato.

- Delimitación de responsabilidades en la empresa: que comenzarán tras una evaluación de las necesidades departamentales y requerirá de la implementación de los planes de acción aplicables.

Estas buenas prácticas deberían provenir de sujetos diferentes. Al aludir a la responsabilidad conjunta no se plantea ese compromiso desde el establecimiento de roles, sino que se presupone de forma previa, movido por un impulso de mejora que nazca del conocimiento de la propia área. La dirección de la empresa, los responsables de cada área, el Departamento de IT. Todos son responsables y al mismo tiempo es complicado reunir en un solo sujeto la responsabilidad de desarrollar estas iniciativas, por lo que el esfuerzo común se traducirá en agilidad, mejores resultados y prematura consecución de los objetivos encaminados a garantizar la integridad de los datos.

Roles y responsabilidades en la seguridad de la información

Los roles y las responsabilidades que se estructuran en torno a la seguridad de la información presentan una dicotomía que obedece a su origen. Dependiendo de si su procedencia se encuadra en un ámbito externo a la organización, como es el caso de los proveedores de servicio; o si reside en el interior de la misma, sus competencias variarán, pese a compartir objetivo: velar por la integridad del dato en último término.

Seguridad de la información en un ámbito externo a la organización: proveedores de servicio

La responsabilidad de los proveedores de servicio, como representantes más comunes de las figuras externas a la organización que pueden interactuar con su información, creando una brecha de seguridad, se resume en forma de documento. Los acuerdos de nivel de servicio establecen los objetivos que deben guiar y que comprometen a estas empresas de IT en modalidad de outsourcing, definiendo su responsabilidad en cuanto a protección de datos. Los aspectos básicos que esta declaración de compromiso debe comprender son:

- Control de las tecnologías, y también de su funcionamiento.
- Realización de copias de seguridad, que actúen como un respaldo.
- Implementación de procesos de recuperación, para poner en marcha caso de que fuese necesario.

Debe tenerse en cuenta que los propietarios de los sistemas, los dueños y encargados de la información, no quedan exentos de su responsabilidad en materia de seguridad de la información ya que en ellos recaerán otras obligaciones, como todas las relativas a la administración y gobierno de datos, imprescindibles para mantener la integridad de los datos en la organización dentro de los estándares deseados.

Seguridad de la información en un ámbito interno a la organización: área de IT interna

Aunque el área de IT se encuentra externalizada en numerosas ocasiones, también existen empresas que cuentan con su propio Departamento de IT. En él se encontrarían las figuras de jefe de seguridad, DBA y arquitecto de datos. El objetivo de integridad de datos está muy ligado a este área pero, lejos de pertenecer a ella o concentrar aquí todas las responsabilidades derivadas, debería extrapolarse a los distintos departamentos afectados. Esta visión es especialmente importante cuando hablamos de fallos de integridad o errores humanos y, por eso, es fundamental que, como roles y responsabilidades, cada área se responsabilice de su parcela, de su producción, de su ámbito de competencias. Teniendo siempre la opción de acudir a IT si se presenta algún problema. Todos los miembros de la organización son responsables de lo que hacen, lo que consumen y lo que producen.

Datos externalizados seguros e íntegros

Una de las claves más importantes a la hora de preservar la integridad de los datos es el afrontar la externalización de los mismos. Cada día, cada minuto se generan datos en las empresas. Gran parte de esta información se consume internamente pero también son muchos los datos que se envían al exterior, como pueden ser:

- **Datos relativos al personal:** cuando se trabaja con empresas de selección o ETTs.
- **Información fiscal:** en los casos en que se cuenta con el apoyo de una gestoría.
- **Datos relativos a las ventas y al stock:** si el escenario planteado incluye áreas de retail.
- **Información relativa al abastecimiento:** cuando se tiene externalizado como área.

Seguridad e integridad: el objetivo a alcanzar en datos externalizados

La realidad es que la mayoría de las compañías comparte sus datos con empresas externas, proporción que se multiplica en los casos de los proveedores de TI. Como comentábamos en el capítulo anterior, esta configuración de la organización genera de por sí una brecha de seguridad en los datos que puede afectar su integridad. De hecho, cualquier política que implique el no trabajar con los datos de manera interna exclusivamente, sino también enviarlos al exterior, independientemente del tipo de canal utilizado, causa una brecha de seguridad que requiere de una protección especial. Sería el caso de:

- Exportar información de tu empresa a otra empresa.
- Exportar datos dentro de tu empresa desde un departamento/sección/país a otro distinto.
- Y también los casos en que, desde dentro de tu propio departamento, envías datos a la nube.

Las consecuencias de la pérdida de seguridad de la información, o de la falta de integridad de los datos, pueden afectar a la compañía de forma interna, pero también en su proyección al exterior tanto a nivel de imagen, como en cuanto a sus relaciones con clientes y proveedores; pudiendo, en el peor de los casos, acarrear incluso consecuencias legales, si los datos filtrados revelan información sensible del negocio.

Por eso es importante que se disponga de políticas de seguridad tanto para ambientes productivos, como para las áreas de desarrollo y test que hacen uso de estos datos, de forma que se pueda trabajar con esa información pero en base a datos enmascarados, asociados a un determinado nivel de autorización o perfil de usuario, que garantizan su seguridad e integridad.

Medición de la integridad de datos

La importancia de medir la integridad de los datos radica en la capacidad de disponer de datos fiables con garantías. Las métricas son necesarias para conocer dónde estamos, discernir cuál es el camino a seguir y detectar pérdidas de alineación de forma temprana, cuando todavía se dispone de un margen de tiempo que posibilita la reacción.

Las mediciones sobre la integridad del dato per se, o sobre la integridad como atributo de la calidad del dato, suelen condensarse en proyectos de calidad. Esta particular configuración hace necesario definir el desarrollo de los mismos en base a la mejora continua. Actuar de esta manera, estableciendo una periodicidad y sistematizando el seguimiento, contribuye decisivamente a mejorar la alineación.

Estas mediciones periódicas han de planearse, ejecutarse y supervisarse por parte de los expertos de cada departamento, los dueños de los datos. La medición de la integridad de los datos requiere de la asunción de responsabilidades, partiendo de un compromiso previo que distribuya las competencias de cada encargado de los datos, en base a sus roles. En esta etapa de medición, la calidad del dato durante el ciclo de vida juega un papel fundamental.

Los indicadores clave para medir la integridad de los datos

Las métricas más utilizadas para practicar las mediciones de la integridad de los datos y garantizar su unicidad son:

- **Precisión de los datos:** que cada dato sea fiel representante de lo que la función que se le atribuye requiere, haciéndolo de la forma establecida.
- **Confiabilidad de los datos:** dotando a la información de coherencia y estabilidad.
- **Completitud de los datos:** que garantice que ni en los propios datos ni en los registros o tablas donde se almacenan falten campos ni valores, que todo esté completo.
- **Conformidad:** referida a un formato, que ha de respetarse a la hora de ingresar el dato y cuyas condiciones se han dispuesto de manera específica y predeterminada.
- **Consistencia:** que relaciona los datos con las reglas de negocio existentes, garantizando que, además de que el dato es correcto en cuanto a sus atributos, no vulnera ninguna.

La calidad de los datos también importa

Implementar un proceso de mejora de datos en la empresa es de gran utilidad, incluso para las organizaciones que no alcanzan una comprensión clara de los mismos o que carecen de un determinado perfil tecnológico. En Powerdata hemos comprobado, desde nuestra experiencia, que los negocios que buscan garantizar la integridad de sus datos y se preocupan por su calidad necesitan empaparse de este concepto, para poder exportarlo a todos los niveles de su organigrama.

La consecución de objetivos, en concreto del de calidad, requiere de la participación activa, responsable y comprometida de todos quienes intervienen, de una u otra forma, sobre el ciclo de vida del dato. Ya sea porque los generan, porque los consumen, porque los dotan de una estructura... el rol en sí, de forma aislada no tiene un sentido completo, ya que requiere de una concepción conjunta que globalice su relevancia, para optimizar la eficacia de cada actuación individual, minimizando el riesgo.

4 pistas para averiguar en qué consiste la calidad del dato

Es importante aclarar, llegados a este punto, que la calidad de los datos no sólo se refiere a la ausencia de defectos. Un dato puede ser completo pero puede estar falto de otras cualidades, imprescindibles para su misión; o puede ser confiable pero necesitar de la dirección correcta, que lo encuadre debidamente permitiendo a su usuario sacar rendimiento a su consumo. Por eso, la calidad del dato, tan unida al concepto de integridad, se articula en base a:

- **La visión única:** que los datos deben proporcionar.
- **La relación e interrelación:** con todas las fuentes y sistemas, siempre de la manera correcta.
- **La consistencia, completitud y adecuación de los datos:** en cuanto a su función.
- El cumplimiento de normativas y leyes, porque las organizaciones no son entes aislados, sino que se encuadran en una sociedad que cuenta con sus propias reglas.

Todo proceso de mejora de datos requiere de mediciones, ya que sólo de esta forma es posible aspirar a garantizar la calidad del dato. El papel que la integridad juega en un proyecto de este tipo, desde su posición de atributo de la calidad, es indicar que los datos son totalmente coherentes.

La importancia del gobierno de los datos

Tener control sobre el ciclo de vida del dato es la clave para evitar problemas de integridad. El primer paso consiste en conocer la trazabilidad, algo imprescindible para alcanzar y comprender cómo trabaja el dato dentro de la empresa, qué caminos sigue la información en su flujo continuo. Lograr estos necesarios conocimientos y control es la finalidad del gobierno de datos.

Las 6 áreas fundamentales para el gobierno de datos

Los elementos clave del gobierno de datos pueden clasificarse en seis categorías básicas:

- **Accesibilidad:** que guíe hacia la visión única desde una perspectiva global.
- **Disponibilidad:** porque es necesaria una máxima actualización, al ser la agilidad más un requisito que una opción.
- **Calidad:** indispensable para tomar la confiabilidad del dato como punto de partida.
- **Coherencia:** íntimamente relacionada con la integridad de la información.
- **Seguridad:** que garantice que no existen filtraciones ni accesos no permitidos a los datos.
- **Verificabilidad:** de los datos mediante auditorías.

Tecnología y gobierno de datos

El adecuado uso de tecnología es importante en tanto en cuanto presenta un marco integral para la gestión y el gobierno de datos. Si el Data Governance es débil, atraerá problemas de calidad e integridad de datos, que se traducirán en malas decisiones, un problema a evitar sin duda alguna.

Sin embargo, generalmente el gobierno de datos no es el correcto porque las empresas no lo toman en cuenta como concepto. Lo habitual es encontrar que las organizaciones funcionan de manera aislada, estructurando el conocimiento de la información y el control sobre los datos por departamentos o por sistemas. Encerrarse en esa administración aislada en vez de comprenderla como un conjunto, como un todo, e ignorar el carácter decisivo del gobierno de datos es lo peor que se puede hacer, y la vía más directa hacia la pérdida de cohesión y coherencia.

Conclusión

La integridad de los datos es un punto crítico en la gestión de la información. La alineación con la estrategia de la organización o el incremento de los niveles de seguridad de la información son sólo algunas de las bondades de que se pueden beneficiar quienes conocen y controlan este atributo de la calidad del dato. Medición y automatización ponen en el camino correcto para la integración de sistemas y confiabilidad de los datos en un entorno de cohesión.

En base a su importancia, puede concluirse que:

- La regla GIGO (Garbage in – Garbage out): que afirma que la introducción de datos erróneos genera resultados erróneos, tiene la misma vigencia hoy que cuando fue formulada, hace 60 años. La diferencia entre aquella época y la actual, a este respecto, sólo radica en el crecimiento exponencial del volumen de los datos digitales.
- La no aplicación de métricas sobre la integridad de los datos: debería considerarse un obstáculo.
- En la medida en que el gobierno de datos no reciba un grado de atención adecuado: las organizaciones estarán expuestas a graves riesgos que podrían afectar a sus operaciones, su situación financiera, su capacidad de cumplimiento y su reputación.
- La meta debe ser combinar tecnología con normas y buenas prácticas de forma fluida y sin estridencias.

PowerData

PowerData, es una compañía multinacional de origen español con gran presencia regional, está enfocada en todo lo relacionado con la Gestión y Gobierno de Datos, tiene una trayectoria de más de 20 años impulsado una cultura Data-Driven en las empresas de la mano de sus aliados tecnológicos.

Te invitamos a explorar los proyectos donde aportamos valor con la gestión de datos. powerdata.es