

GIGO, calidad de datos y control en Sistemas de Información

Presentación del tema

En Tecnologías de la Información, uno de los principios más simples y, al mismo tiempo, más importantes es GIGO (*Garbage In, Garbage Out*, “basura entra, basura sale”). La idea central es directa: si un sistema recibe datos incorrectos, incompletos, inconsistentes o mal definidos, sus resultados también serán incorrectos, incompletos, inconsistentes o poco útiles.

Este principio no depende de la antigüedad o modernidad del sistema. Se aplica a una planilla de cálculo, a un sistema contable, a un ERP (*Enterprise Resource Planning*, sistema de planificación de recursos empresariales), a una plataforma de comercio electrónico, a un tablero de BI (*Business Intelligence*, inteligencia empresarial) y también a una herramienta de IA (*Artificial Intelligence*, inteligencia artificial). La tecnología puede procesar más rápido, integrar más fuentes y presentar resultados de forma más sofisticada, pero no puede convertir automáticamente datos deficientes en información confiable.

Desde la mirada de las Tecnologías de la Información, GIGO obliga a formular una pregunta administrativa fundamental: ¿qué calidad tienen los datos sobre los cuales se toman decisiones? Para estudiantes de Administración, esta pregunta es especialmente relevante porque muchas decisiones gerenciales se apoyan en reportes, indicadores, presupuestos, tableros, pronósticos y modelos que parecen objetivos, pero que pueden estar contruidos sobre datos débiles.

Un sistema puede funcionar técnicamente y, aun así, producir información administrativamente equivocada. Por ejemplo, una aplicación puede calcular correctamente el total de una factura, pero si el precio unitario cargado es incorrecto, el resultado será incorrecto. Un tablero puede mostrar ventas por región con gráficos claros, pero si los clientes fueron asignados a regiones equivocadas, el análisis será engañoso.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Un modelo de IA puede redactar una respuesta convincente, pero si el pedido del usuario está mal formulado o contiene supuestos falsos, la salida puede ser inadecuada.

El sentido administrativo de GIGO

GIGO no es solo una expresión técnica. Es una advertencia sobre la relación entre datos, información y decisión. En un Sistema de Información, los datos son representaciones básicas de hechos, operaciones o eventos. La información surge cuando esos datos se organizan, procesan e interpretan con un propósito. La decisión aparece cuando esa información se utiliza para elegir un curso de acción.

Si los datos de base son deficientes, la cadena completa se debilita. El problema no queda limitado al área de sistemas. Afecta contabilidad, compras, ventas, logística, recursos humanos, finanzas, auditoría y dirección. Por eso, la calidad de los datos debe ser tratada como un asunto de gestión, control interno y gobierno de TI (*IT Governance*, gobierno de Tecnologías de la Información).

Ejemplo: una empresa decide aumentar la producción porque el sistema muestra crecimiento sostenido de ventas. Sin embargo, luego descubre que una parte de esas ventas correspondía a pedidos duplicados que nunca debieron registrarse. El sistema procesó los datos disponibles, pero la decisión se apoyó en una base defectuosa. En ese caso, el problema no fue solo tecnológico. También fue administrativo, porque fallaron los controles de carga, validación y revisión.

De los datos a la información confiable

Para comprender GIGO conviene diferenciar tres niveles: dato, información y conocimiento. El dato es un valor capturado por el sistema. La información es el dato organizado para responder una pregunta. El conocimiento aparece cuando esa información se interpreta en contexto y permite actuar.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Ejemplo: “125” es un dato aislado. “125 unidades vendidas en la sucursal Norte durante mayo” ya es información. “La sucursal Norte necesita reforzar stock porque su demanda mensual supera el promedio histórico” es conocimiento aplicado a la gestión.

GIGO advierte que este proceso solo funciona si los datos son confiables. Un dato puede ser técnicamente válido, pero administrativamente incorrecto. Por ejemplo, una fecha puede tener formato correcto, pero no corresponder al contrato real. Un número de cliente puede existir en la base, pero estar asociado a la persona equivocada. Un importe puede ser numérico, pero estar cargado en una moneda incorrecta.

Por eso, la calidad de datos no se limita a que el sistema “acepte” el valor ingresado. También exige que ese valor sea correcto, completo, consistente, oportuno, autorizado y útil para el proceso de negocio.

Dimensiones de la calidad de datos

Desde la administración de Tecnologías de la Información, la calidad de datos puede evaluarse mediante varias dimensiones. Estas dimensiones ayudan a diseñar controles y a detectar dónde puede originarse la “basura” que luego afecta al sistema.

Dimensión	Pregunta de control	Ejemplo administrativo
Exactitud	¿El dato representa correctamente la realidad?	El importe de una factura coincide con el comprobante recibido.
Compleitud	¿Falta algún dato necesario?	Una orden de compra incluye proveedor, importe, fecha, centro de costo y aprobación.
Consistencia	¿El dato no contradice otros datos del sistema?	La fecha de baja de un empleado no puede ser

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Dimensión	Pregunta de control	Ejemplo administrativo
		anterior a su fecha de ingreso.
Validez	¿El dato respeta formato, tipo, rango o regla definida?	El CUIT tiene formato correcto y supera la validación correspondiente.
Oportunidad	¿El dato está disponible cuando se necesita?	Las cobranzas del día se cargan antes del cierre de tesorería.
Unicidad	¿El dato no está duplicado indebidamente?	Una factura no aparece dos veces con el mismo proveedor, tipo y número.
Trazabilidad	¿Puede reconstruirse el origen y el cambio del dato?	Se conoce quién modificó la cuenta bancaria de un proveedor y con qué autorización.

Estas dimensiones muestran que GIGO no se resuelve únicamente con tecnología. Requiere reglas de negocio, responsables funcionales, controles automatizados, procedimientos, capacitación y auditoría.

GIGO y controles preventivos

Los controles preventivos son aquellos que buscan evitar que el error, la omisión, el fraude o la inconsistencia ingresen al sistema. Desde la lógica de GIGO, son especialmente importantes porque actúan antes de que el dato defectuoso contamine procesos posteriores.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

En Sistemas de Información, prevenir suele ser más eficiente que corregir. Si una factura se carga con un proveedor equivocado, ese error puede afectar cuentas por pagar, impuestos, reportes de compras, análisis de proveedores y flujo de fondos. Corregirlo después exige tiempo, conciliaciones, autorizaciones y posible revisión de reportes ya emitidos.

Ejemplos de controles preventivos:

- Campos obligatorios que impiden grabar una operación incompleta.
- Validaciones de formato para fechas, identificadores fiscales, códigos postales o cuentas bancarias.
- Listas desplegables que reducen escritura libre y evitan variaciones innecesarias.
- Límites de rango que impiden cargar descuentos superiores a lo autorizado.
- Validación de duplicados para evitar facturas, clientes o productos repetidos.
- Controles de acceso que limitan quién puede crear, modificar o aprobar datos críticos.
- Segregación de funciones para impedir que una misma persona cargue, apruebe y concilie una operación sensible.

Ejemplo: en un sistema de compras, el alta de un proveedor no debería depender solo de que alguien escriba un nombre y una cuenta bancaria. Debería exigir identificación fiscal válida, documentación respaldatoria, condición tributaria, datos bancarios verificados, responsable de carga, aprobación funcional y registro de auditoría. Cada control reduce la posibilidad de que un dato incorrecto ingrese al circuito.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Controles de entrada

Los controles de entrada (*Input Controls*, controles sobre los datos ingresados) son el punto más evidente de aplicación de GIGO. Su finalidad es asegurar que el dato capturado por el sistema sea válido, completo, autorizado y razonable desde el inicio.

Un error de entrada puede parecer pequeño, pero su impacto se multiplica si el sistema lo utiliza en cálculos, reportes, integraciones o decisiones automatizadas. La automatización no elimina el error de origen; muchas veces lo acelera y lo distribuye.

Ejemplo: si se carga mal la alícuota de un impuesto en un sistema de facturación, el sistema puede emitir cientos de facturas técnicamente consistentes, pero fiscalmente incorrectas. El error inicial se transforma en un problema operativo, contable y legal.

Controles típicos de entrada:

Control	Función	Ejemplo
Campo obligatorio	Evita datos incompletos	No se permite registrar una factura sin proveedor.
Máscara de entrada	Obliga a respetar un formato	Fecha con formato día/mes/año.
Validación de tipo	Controla si el dato es texto, número o fecha	Un importe no puede contener letras.
Validación de rango	Evita valores fuera de parámetros	Un descuento no puede superar el máximo autorizado.
Validación contra maestro	Verifica existencia previa	El código de cliente debe existir en la base de clientes.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Control	Función	Ejemplo
Control de duplicidad	Evita registros repetidos	Factura con igual proveedor, tipo y número.
Dígito verificador	Detecta errores de transcripción	CUIT, tarjeta de crédito, IBAN o CBU según reglas aplicables.
Autorización previa	Controla responsabilidad	Alta de proveedor aprobada por un responsable funcional.

Estos controles deben diseñarse con criterio. Si son demasiado débiles, permiten errores. Si son excesivos o mal configurados, dificultan la operación y generan atajos informales. El desafío de TI y Administración es encontrar un equilibrio entre seguridad, eficiencia y usabilidad.

Controles durante la transmisión de información

Los Sistemas de Información no trabajan aislados. En muchas organizaciones, los datos viajan entre aplicaciones, sucursales, bancos, proveedores, clientes, plataformas de comercio electrónico, servicios en la nube y organismos públicos. En ese recorrido también se aplica GIGO: si el dato se altera, se pierde, se duplica o llega incompleto durante la transmisión, el sistema receptor procesará información defectuosa.

Los controles de transmisión buscan asegurar que el dato enviado sea el mismo que el dato recibido y que llegue al destinatario correcto. Estos controles son especialmente relevantes en integraciones, importaciones masivas, archivos bancarios, facturación electrónica, interfaces entre sistemas y APIs (*Application Programming Interfaces*, interfaces de programación de aplicaciones).

Ejemplos de controles de transmisión:

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

- Totales de control para comparar cantidad de registros e importes enviados y recibidos.
- Conteo de registros para detectar faltantes o duplicados.
- Checksums (*checksums*, sumas de verificación) para validar integridad técnica del archivo.
- Cifrado de archivos para proteger información durante el envío.
- Registro de archivos rechazados, reprocesados o reenviados.
- Confirmaciones de recepción por parte del sistema destino.
- Identificación de lote, fecha, hora, usuario y origen del envío.

Ejemplo: una empresa envía al banco un archivo con 850 pagos por un total de 120 millones de pesos. Antes del envío, el sistema debería calcular cantidad de operaciones, importe total y hash o checksum. El banco o sistema receptor debería confirmar esos valores. Si recibe 849 operaciones o un importe distinto, el proceso no debería continuar automáticamente.

Controles de procesamiento

Los controles de procesamiento (*Processing Controls*, controles durante el tratamiento de los datos) verifican que el sistema procese la información de manera completa, exacta, autorizada y secuencial. Aquí GIGO se combina con otra advertencia: incluso si los datos de entrada son correctos, un mal procesamiento puede producir salidas erróneas.

Estos controles son críticos cuando hay cálculos automáticos, cierres contables, liquidación de sueldos, actualización de precios, asignación de stock, importación de cobranzas, generación de intereses, conciliaciones automáticas o integración entre módulos.

Ejemplos de controles de procesamiento:

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Control	Riesgo que reduce	Ejemplo
Total de control	Procesamiento incompleto	Comparar importe total antes y después de importar cobranzas.
Conteo de registros	Faltantes o duplicados	El archivo tenía 3.000 registros y se procesaron 2.997.
Validación de secuencia	Salto o alteraciones	Numeración correlativa de comprobantes.
Conciliación entre módulos	Diferencias entre sistemas	Ventas contra contabilidad.
Revisión de excepciones	Casos fuera de regla	Pagos rechazados, importes negativos o descuentos excesivos.
Bloqueo durante proceso	Cambios simultáneos indebidos	No permitir modificaciones mientras se ejecuta una liquidación.
Bitácora de ejecución	Falta de trazabilidad	Registrar usuario, fecha, parámetros y resultado del proceso.

Ejemplo: antes de liquidar sueldos, el sistema debería validar empleados activos, novedades cargadas, ausencias, horas extras, categorías, deducciones y topes aplicables. Después del proceso, debería emitir totales por concepto, empleados liquidados, importes netos y excepciones. Si un empleado aparece con sueldo negativo o duplicado, el sistema debería impedir el cierre hasta su revisión.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Controles de salida

Los controles de salida (*Output Controls*, controles sobre reportes, archivos y resultados) buscan asegurar que la información producida por el sistema sea completa, correcta, autorizada, protegida y entregada a destinatarios adecuados. Aunque muchas veces se consideran controles detectivos, también cumplen una función preventiva cuando bloquean la emisión de resultados incorrectos o confidenciales.

Una salida puede ser un reporte gerencial, una factura, una orden de pago, un archivo bancario, un tablero de indicadores, un listado de clientes, una exportación de datos o una respuesta generada por un modelo de IA.

Ejemplos de controles de salida:

- Conciliación de reportes con fuentes de datos.
- Revisión de totales antes de emitir archivos externos.
- Clasificación de información como pública, interna, confidencial o crítica.
- Restricción de impresión, descarga o reenvío de reportes sensibles.
- Distribución segura a destinatarios autorizados.
- Registro de emisión de reportes, usuario, fecha y versión.
- Reportes de excepción para identificar datos fuera de parámetros.

Ejemplo: un tablero de ventas mensual debería indicar fuente de datos, fecha de actualización, filtros aplicados y alcance del reporte. Si el tablero excluye ventas anuladas, operaciones pendientes o una sucursal determinada, esa condición debe estar clara. De lo contrario, la gerencia podría interpretar el resultado como si representara la totalidad del negocio.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

GIGO, BI y tableros de control

En BI (*Business Intelligence*, inteligencia empresarial), GIGO se vuelve especialmente visible. Los tableros de control suelen presentar indicadores de forma gráfica, ordenada y aparentemente objetiva. Esa presentación puede generar confianza excesiva, incluso cuando los datos de origen tienen problemas.

Un gráfico bien diseñado no garantiza información correcta. Un indicador puede estar visualmente claro y metodológicamente mal construido. Por eso, antes de usar un tablero para decidir, la organización debe conocer la fuente de datos, la definición del indicador, la frecuencia de actualización, las reglas de depuración, los filtros aplicados y las responsabilidades sobre la calidad.

Ejemplo: un indicador de “clientes activos” puede variar según la definición adoptada. Para ventas, puede ser cliente que compró en los últimos 90 días. Para cobranzas, puede ser cliente con cuenta abierta. Para marketing, puede ser cliente que interactuó con una campaña. Si el tablero no define el concepto, las áreas pueden discutir decisiones usando la misma palabra con significados distintos.

Desde TI, esto exige gobierno de datos (*Data Governance*, gobierno de datos), diccionarios de datos, definiciones comunes, dueños funcionales y controles de calidad antes de publicar indicadores.

GIGO y auditoría de Sistemas de Información

La auditoría de Sistemas de Información utiliza el principio GIGO para evaluar si los controles permiten confiar en los datos y resultados del sistema. No basta con verificar que una aplicación exista o que un reporte se emita. Es necesario revisar cómo se originan los datos, quién los autoriza, qué validaciones existen, cómo se procesan, qué excepciones aparecen y qué evidencia queda.

Una auditoría orientada por GIGO puede formular preguntas como las siguientes:

- ¿Qué datos críticos ingresan al sistema?

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

- ¿Quién puede cargarlos, modificarlos o eliminarlos?
- ¿Qué controles impiden errores de formato, rango, duplicidad o inconsistencia?
- ¿Existen controles sobre integraciones, importaciones y transmisiones?
- ¿Qué bitácoras o pistas de auditoría permiten reconstruir cambios?
- ¿Los reportes se concilian contra fuentes confiables?
- ¿Hay responsables funcionales por la calidad de los datos?
- ¿Se revisan excepciones o solo se acumulan en reportes que nadie mira?

Ejemplo: en un sistema de pagos, la auditoría debería revisar altas de proveedores, cambios de cuentas bancarias, aprobaciones, segregación de funciones, registros de modificación, archivos enviados al banco y conciliación posterior. El objetivo es verificar que los datos que originan pagos sean confiables antes de que el dinero salga de la organización.

GIGO en Inteligencia Artificial

El principio GIGO adquiere una nueva importancia en la IA (*Artificial Intelligence*, inteligencia artificial), especialmente en la IA generativa (*Generative Artificial Intelligence*, inteligencia artificial generativa). Los modelos de lenguaje pueden producir textos, resúmenes, respuestas, análisis, código o propuestas a partir de instrucciones del usuario. Sin embargo, la calidad de la salida depende en gran medida de la calidad de la entrada.

En este contexto, la entrada no es solo un dato numérico. También puede ser una pregunta, una instrucción, un documento, una consigna, una base de datos, una imagen, una transcripción o un conjunto de restricciones. Si esa entrada es ambigua, incompleta, contradictoria o insuficiente, la respuesta de la IA puede ser superficial, errónea o poco aplicable.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Ejemplo: pedirle a una IA “haceme un informe de ventas” es una instrucción débil. No indica período, fuente, unidad de análisis, moneda, región, público destinatario, formato, objetivo ni criterios de interpretación. Una respuesta generada con esa entrada puede parecer razonable, pero difícilmente sea útil para una decisión administrativa concreta.

Un prompt (*prompt*, instrucción o pedido dado a un modelo de IA) de mejor calidad podría indicar: “Analizá las ventas del primer trimestre por región, comparalas contra el mismo período del año anterior, destacá variaciones superiores al 10 %, separá efectos de precio y cantidad cuando sea posible, y prepará conclusiones para gerencia comercial en formato ejecutivo”. Esta entrada define objetivo, alcance, comparación, criterio de análisis y destinatario.

Ingeniería de prompts como control de entrada

La ingeniería de prompts (*Prompt Engineering*, diseño sistemático de instrucciones para modelos de IA) puede entenderse como una forma moderna de control de entrada. Así como un sistema administrativo necesita campos obligatorios, validaciones y reglas de negocio, una interacción con IA necesita instrucciones claras, contexto suficiente y criterios de salida.

Un buen prompt no consiste solo en escribir más. Consiste en estructurar mejor el problema. Debe aclarar qué se busca, desde qué rol se debe responder, qué información debe utilizarse, qué límites existen, qué formato se espera y cómo se evaluará la calidad del resultado.

Elementos recomendables de un prompt:

Elemento	Función	Ejemplo
Objetivo	Define qué se quiere lograr	“Preparar un resumen ejecutivo”.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Elemento	Función	Ejemplo
Contexto	Sitúa el problema	“Para estudiantes de licenciatura en administración”.
Rol	Orienta la perspectiva	“Respondé desde la mirada de Tecnologías de la Información”.
Alcance	Delimita qué incluir o excluir	“No incluyas aspectos legales salvo los vinculados a control de datos”.
Formato	Ordena la salida	“Usá subtítulos, ejemplos y preguntas de autoevaluación”.
Criterios	Define calidad esperada	“Lenguaje académico, claro y aplicable”.
Fuentes o datos	Reduce arbitrariedad	“Basate en el texto proporcionado y no inventes cifras”.

Desde Administración, esto implica que usar IA también requiere control. No alcanza con conocer la herramienta. Hay que saber formular problemas, revisar resultados, validar supuestos, contrastar fuentes y asumir responsabilidad por la decisión final.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Riesgos de GIGO en IA generativa

La IA generativa puede amplificar el problema de GIGO porque sus salidas suelen tener forma convincente. Un texto bien redactado puede ocultar una entrada pobre. Esto genera un riesgo administrativo: confundir fluidez con confiabilidad.

Riesgos frecuentes:

- Prompts ambiguos que producen respuestas generales.
- Datos incompletos que generan conclusiones parciales.
- Supuestos no declarados que orientan mal el análisis.
- Fuentes no verificadas que debilitan la evidencia.
- Indicaciones contradictorias que producen resultados inconsistentes.
- Falta de revisión humana en decisiones sensibles.
- Uso de información confidencial en herramientas no autorizadas.

Ejemplo: una organización puede pedir a una IA que analice reclamos de clientes, pero si carga solo reclamos de un canal y excluye llamadas telefónicas, correos o redes sociales, la conclusión será sesgada. El modelo puede encontrar patrones en los datos disponibles, pero no puede compensar por sí solo la ausencia de información relevante.

Por eso, en IA también deben existir controles: selección de datos, anonimización cuando corresponda, revisión de privacidad, definición de alcance, validación humana, evaluación de sesgos, registro de versiones y trazabilidad del uso.

Ejemplos integradores desde Administración y TI

Sistema de facturación

Una empresa implementa un sistema de facturación que toma precios desde una tabla maestra de productos. Si el precio se carga mal, todas las facturas posteriores serán

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

incorrectas. El control preventivo consiste en limitar quién puede modificar precios, exigir aprobación, registrar cambios y generar un reporte de variaciones. GIGO muestra que el problema no está solo en la factura emitida, sino en el dato maestro que alimenta el proceso.

Sistema de inventario

Un depósito utiliza lectores de código de barras para registrar entradas y salidas. Si los productos están mal codificados, el sistema puede descontar unidades de otro artículo. El tablero de stock mostrará información formalmente calculada, pero materialmente incorrecta. El control requiere validación de códigos, conteos físicos, conciliación periódica y trazabilidad de movimientos.

Sistema de recursos humanos

Un sistema de liquidación de haberes calcula sueldos según categoría, antigüedad y novedades. Si una novedad de ausencia se carga en el empleado equivocado, la liquidación será incorrecta. El sistema puede aplicar bien la fórmula, pero sobre un dato equivocado. Los controles deben incluir revisión de novedades, autorización por responsable y reporte de excepciones.

Tablero gerencial

La dirección observa un tablero que muestra caída de rentabilidad. Sin embargo, el indicador combina ventas netas con costos de reposición de distintos períodos. La visualización es atractiva, pero la metodología es inconsistente. Desde GIGO, el problema está en la definición del indicador y en la integración de datos, no en el gráfico.

IA para atención al cliente

Una empresa usa IA para responder reclamos frecuentes. Si la base de conocimiento está desactualizada, el modelo puede responder con políticas vencidas. El problema no es solo del modelo, sino del insumo informacional. Se necesitan controles sobre actualización de

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

contenidos, aprobación de respuestas, monitoreo de casos críticos y escalamiento a personas cuando corresponda.

Criterios para aplicar GIGO en proyectos de TI

En un proyecto de Sistemas de Información, GIGO debe considerarse desde el análisis inicial, no al final. Es necesario identificar datos críticos, fuentes, responsables, reglas de validación, controles, excepciones y mecanismos de corrección antes de poner el sistema en producción.

Criterios prácticos:

- Identificar qué datos son críticos para el proceso de negocio.
- Definir dueños funcionales de esos datos.
- Documentar reglas de calidad, validación y autorización.
- Diseñar controles de entrada, transmisión, proceso y salida.
- Evitar duplicación innecesaria de datos maestros.
- Incorporar pistas de auditoría para cambios sensibles.
- Establecer reportes de excepción revisables.
- Capacitar a usuarios en carga y revisión de datos.
- Medir calidad de datos con indicadores.
- Revisar periódicamente controles y corregir causas, no solo síntomas.

Este enfoque muestra que la calidad de la información no aparece espontáneamente. Se diseña, se controla, se mide y se gobierna.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Ideas clave

GIGO recuerda que un sistema de información no es confiable solo porque sea moderno, rápido o automatizado. La confiabilidad depende de la calidad de los datos, de los controles aplicados y de la responsabilidad administrativa sobre el ciclo completo de la información.

Desde Tecnologías de la Información, GIGO conecta calidad de datos, control interno, auditoría, seguridad, BI, gobierno de datos e inteligencia artificial. En todos los casos, la pregunta central es la misma: ¿los insumos informacionales permiten producir resultados confiables?

Para estudiantes de Administración, el aprendizaje principal es que no se debe aceptar un reporte, un tablero, una salida del sistema o una respuesta de IA sin comprender cómo se generó. La administración responsable exige mirar detrás del resultado: qué datos entraron, quién los cargó, qué controles se aplicaron, cómo se procesaron y qué evidencia permite confiar en ellos.

Preguntas de autoevaluación

1. ¿Qué significa GIGO y por qué es un principio central en Sistemas de Información?
2. ¿Por qué un sistema técnicamente correcto puede producir información administrativamente incorrecta?
3. ¿Qué diferencia existe entre dato, información y conocimiento aplicado a la gestión?
4. ¿Cuáles son las principales dimensiones de la calidad de datos?
5. ¿Por qué los controles preventivos son especialmente importantes desde la perspectiva de GIGO?

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

6. ¿Qué ejemplos de controles de entrada pueden aplicarse en un sistema de compras?
7. ¿Qué riesgos aparecen durante la transmisión de información entre sistemas?
8. ¿Cómo ayudan los totales de control y conteos de registros a proteger la integridad de un proceso?
9. ¿Por qué los controles de salida son relevantes para reportes gerenciales y archivos externos?
10. ¿Cómo puede un tablero de BI generar decisiones erróneas aunque tenga buenos gráficos?
11. ¿Qué función cumple el gobierno de datos en la prevención de GIGO?
12. ¿Por qué la ingeniería de prompts puede entenderse como un control de entrada en IA?
13. ¿Qué elementos debería incluir un prompt de calidad para obtener una respuesta útil?
14. ¿Cuáles son los principales riesgos de GIGO en IA generativa?
15. ¿Por qué la revisión humana sigue siendo necesaria aunque se utilicen modelos avanzados de IA?
16. ¿Qué controles aplicaría en un sistema de facturación para evitar errores de precios?
17. ¿Cómo se relacionan GIGO, auditoría de sistemas y trazabilidad?
18. ¿Qué diferencia existe entre corregir un dato erróneo y corregir la causa que permitió su ingreso?

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

19. ¿Por qué la calidad de datos debe considerarse una responsabilidad organizacional y no solo técnica?
20. ¿Cómo aplicaría el principio GIGO al análisis de un proyecto de transformación digital?