MDB 301 – Gobernanza de la Información

Examen I

Estudiante: *Alejandro Marin Badilla*

Profesor: *Claudio Valverde*

Universidad CENFOTEC

Addison, Texas

Octubre 29, 2016

Contenido

De acuerdo con Berson (2011) – Cap. 12

Demuestre lo importante que es un caso de negocio para que una empresa gestione sus datos – 4p

El postulado general de Benson se reduce de que antes de poder iniciar un proceso de gestión de datos hay que tener idea precisa de las condiciones actuales, así como de los resultados esperados. De otras maneras, sin una idea clara del costo de la información de mala calidad, es difícil mantener el soporte de las piezas claves de la organización, ejecutivos y custodios de la información.

De esta manera, por ejemplo, antes de iniciar un proceso de limpieza de la información, por ejemplo de las direcciones de clientes, es importante establecer una idea general de los problemas de datos existentes. Algunas mediciones básica por ejemplo, de la completitud de la información, por ejemplo, la proporción de los campos considerados claves están poblados respecto a la población en general o los niveles de duplicación que existen en las cuentas, nos pueden brindar una idea del beneficio esperado.

Información sobre la completitud se puede evaluar generalmente considerando la población total. Por ejemplo, contar de todas las direcciones disponibles, cuantas incluyen el código postal completo vs. las que no, puede calcularse relativamente fácil para toda la población.

Por otra parte, el costo de los datos duplicados, es más difícil de estimar, y por lo tanto, es muy probable que se deba recurrir técnicas de muestro estadístico, para establecer una muestra representativa. El modelo de la distribución normal y la variabilidad entre la información, permite estimar tamaños de muestra representativos. Establecida estas muestra, se puede proceder con métodos basado en herramientas de calidad de datos, a investigar la frecuencia con que la información está repetida o presenta errores parciales en su presentación.

De esta manera, Berson explica que el impacto de los beneficios se pueden mostrar utilizando dos metodologías:

a) El método tradicional, de vista desde arriba: bajo este método se cuantifican los beneficios evaluando a profundidad el estado actual de proceso, identificando sus ineficiencias y desarrollando un modelo de retorno sobre la inversión para demostrar como el MDM puede reducir los costos e incrementar los ingresos (Berson & Dubov, 2007).
b) El método menos tradicional de estimación del valor económico: este método proveen un estimado de alto nivel del impacto sobre el negocio del MDM y otras iniciativas centradas en la información (Berson & Dubov, 2007).

Relate la importancia que tiene un plan de trabajo para la gestión de datos – 4p

De acuerdo a Berson, la forma más simple de comprender el impacto de un plan de trabajo, es considerar el efecto que su ausencia tiene para un proceso de MDM, de esta manera, sus ideas principales son (Berson & Dubov, 2007):

- Sin un plan de trabajo detallado no es posible estimar de forma inteligente el costo del programa de MDM y cuando dichos costos van a ser incurridos. Sin una información detallada del costo, no es posible hacer balance contra sus beneficios esperados y sobre la situación de flujo de efectivo de la compañía.
- Sin un plan de trabajo, no es posible proveer la perspectiva del tiempo. Se ha discutido en muchos textos, particularmente en (Fisher, 2009) que los procesos de gobernanza de la información y de MDM, son esfuerzos continuos y permanentes. Es la posición de Berson, que al menos debe darse una perspectiva de los primeros cinco años, estableciendo mucho más detalle en el primer año de los logros y las metas, pero sin dejar de lado los objetivos de mayor plazo.
- El plan de trabajo, permite establecer un balance entre la necesidad de tener el suficiente detalle inicial para estimar los costos de puesta en marcha y ejecución en el corto y el mediano plazo evitando al mismo tiempo el riesgo de tratar de llegar a niveles de detalles que no son posibles sin haber iniciado el análisis y la investigación. De esta manera, el plan al menos debe proveer información de las áreas consideradas de mayor impacto y donde deben priorizarse los esfuerzos iniciales. De la misma forma, definir problemas que son alcanzables en el corto plazo es fundamental, para que el mismo éxito del programa de MDM crear una retroalimentación positiva, que le permita obtener los recursos para atacar luego los problemas más complejos.
- Finalmente, las consideraciones de costo relativas al tamaño de la compañía y de la cartera de clientes es fundamental, para establecer la estrategia de trabajo. Algunos estudios han revelado, que por ejemplo, para compañías con clientes en el orden de los 5 millones, el costo de un programa de MDM alcance fácilmente los 3 millones de dólares, considerando los costos de licenciamiento, equipo de procesamiento, el personal que operará los sistemas y desarrollara la integración. Estos además deben estimarse a lo largo de un proceso estimado de al menos 3 a 5 años de operación. De la misma forma, los impactos positivos deben estimarse dentro de estas perspectivas de tiempo.

De acuerdo con el artículo “Strengthening Information Security Governance” explique el eje central sobre lo que el autor escribe - 4p

El punto de partida del doctor Gelbstein, es que al igual que en la instalación de sistemas de alarma en las casas, en vez de que éxista un requisito de la asegurada, o en nuestro caro, un requerimiento de gobernanza mediante una ley, las personas, al igual que las empresas, “solamente consideran instalar las alarmas una vez que han sido objetivo de un robo” (Ed Gelbstein, 2012).

Vista de esta manera, el autor dedica el artículo a establecer que existen 8 motivadores principales por los cuáles se da una débil o inexistente gobernanza de la seguridad de la información (Ed Gelbstein, 2012):

1. Los límites de la seguridad de la información: mientras que los departamentos de tecnología de información pueden proveer guías relacionadas con políticas, estas deben ser revisadas, aprobadas por otros grupos: recursos humanos, la consejería legal e incluso representantes laborales (sindicatos).
2. Falta de interés de parte de los ejecutivos y administradores senior: los ministros, diplomáticos y administradores senior tiene un tiempo disponible valioso y limitado, lo cual los fuerzo a concentrarse en asuntos cuya importancia se limita al aquí y al ahora. “Ellos no pierden el sueño por fallas a la vulnerabilidad de la información, al menos no hasta que están ocurren, […] y en ese caso, su reacción es, corríjanlo” (Ed Gelbstein, 2012). Una vez que el problema de corto plazo ha sido corregido, su interés se evapora y el pensamiento de que la unidad de TI está manejándolo vuelve a restablecerse. Esta situación se ve compuesta por la percepción que tiene la organización de que los administradores de seguridad de la información son los “No, no señor” de la organización.
3. Apetito de riesgo pobremente definido: los riesgos de impacto a los organizaciones cubren más allá de los impactos negativos sobre las operaciones y la entrega de servicios, sino que también afectan a las actividades generadoras de valor asociadas a las oportunidades de negocio o mejoras operativas perdidas por falta de uso de la tecnología. Los términos “apetito del riesgo” y “tolerancia de riesgo” son mal entendidos y utilizados de forma intercambiable. El apetito de riesgo se define como “cuanto riesgo está la organización dispuesta a asumir antes de tomar acciones para mitigarlo […] y poner los recursos a disposición para implementar tales acciones (Ed Gelbstein, 2012)”.
4. Mentalidad de silo: esto, particularmente, porque más allá de los departamentos de TI, una gran cantidad de actores y partes de la empresa requieren comprometerse con el logro de los objetivos de seguridad. El Dr. Gelbstein presenta una lista de 6 actores y otros que no voy a repetir, pero que basta destacar que en una gran actividad común.
5. Uso de políticas de seguridad inefectivas: “las políticas de seguridad son esencialmente una lista de reglas de lo que debe o no hacerse. En un mundo perfecto, el desarrollo de dichas políticas debería hacer a los administradores senior conscientes y envueltos en la seguridad de la información y hacer de ella una prioridad apropiada” (Ed Gelbstein, 2012). Para ser efectiva, las políticas deben ser

entendidas por todos aquellos que necesitan cumplir con ellas y deben ser puestas en marcha de forma efectiva. Más importante, debe haber formas de garantizar que se lleven a la práctica. En muchas organizaciones, para hacer las cosas más difíciles, muchas veces no se sabe con claridad quien es el dueño del proceso de creación de las políticas, de diseminarlas y de monitorear su cumplimiento (Ed Gelbstein, 2012).

6. La revolución del usuario final: “cuando la organizaciones seleccionaban, instalaban y proveían el equipo y el software a sus fuerzas de trabajo […] era relativamente posible monitorear quién así que en el ambiente digital” (Ed Gelbstein, 2012). La revolución en la disponibilidad de recursos tecnológicos de bajo costo, muchas veces provistos por los mismos empleados han aumentado el nivel de complejidad de esta seguridad. Esto ha producido que las arquitecturas de seguridad corporativa se salgan de control y que los usuarios demanden acceso a los sistemas corporativos utilizando sus propios dispositivos, esto compuesto por la revolución del Web 2.0 difumina los límites entre las actividades profesionales y personales.
7. La velocidad de la innovación: la velocidad de la innovación y el aumento de los vectores de ataque lleva a la situación dónde “ninguna organización es invulnerable, el optimista se limita a afirmar que ‘nada es tan malo nunca que no podría ponerse peor’” (Ed Gelbstein, 2012).
8. La falta de habilidad de asignar el valor a la información: las infraestructuras de información crítica, por regla general, tiene mayor probabilidad de poder medir el impacto a la inseguridad, al utilizar técnicas como la medición del impacto del tiempo fuera de servicio. Esto es mucho más difícil de estimar cuando se trata de eventos donde se afecta la seguridad de la información, por ejemplo, cuando se trata de secretos tecnológicos, algunos de los cuales pueden recuperarse de forma efectiva por vía judicial, pero en otras, incluso este medio no permite una recuperación razonable frente a los impactos recibidos.

De acuerdo con Hill (2009) – Caps. 1 a 8:

Describa lo que es la protección de datos - 3p

Hill señala que una de las perspectivas clásicas para considerar la protección de datos, es verlo como un "***costo de hacer negocios***", es decir cómo una función que debe hacerse, contrastadas con las funciones que desea hacerse, que son aquellas que logra los objetivos organizacionales, y de ahí, la importancia de administrar los costos, ya que la inversión en el proceso de protección de datos, disminuye la rentabilidad de la organización (Hill, 2009).

También ofrece la perspectiva alternativa de considerarlo como una "***póliza de seguro***". De tal manera, la protección de datos de tienen como objetivo la maximización de la utilidad o la minimización de los costos, sino "**minimizar las pérdidas ante los peores escenarios de pérdida**", en otras palabras, es un costo necesario de hacer negocios de forma prudente. Este tipo de aseguramiento (póliza) se rige por el principio de minimizar el costo maximizando el valor del seguro (Hill, 2009).

La tecnología no es una situación *deus ex machina*. Los usuarios y sus ejecutivos deben poner en marcha las 4 P de la administración de procesos: política, procesos, procedimientos y prácticas. La tecnología habilita dichos componentes, pero no los remplaza (Hill, 2009).

- **Política**: define el curso de acción, no las acciones.
- **Procesos**: define las acciones a tomar para lograr los objetivos.
- **Procedimientos**: definen las acciones paso por paso, hacen que las políticas conduzcan a acciones.
- **Prácticas**: garantizan que los procedimientos que cumplen con las políticas sean llevados a cabo.

Analice la importancia de la protección de datos - 3p

El marco de referencia de Protección de Datos moderno, ha evolucionado sobre los conceptos de Gobernanza, administración del riesgo y cumplimiento, y Hill señala al Open Compliance and Ethics Group (GRC) cómo una de las organizaciones partidarias de dichos conceptos de mayor visibilidad, quién propone un “desempeño basado en principios” o “principled performance” (Hill, 2009).

Hill percibe que se pueden identificar 3 direcciones desde las cuáles se ha producido un cambio en los requerimientos de protección de datos:

1. La mejora de las capacidades de la tecnología existente, por ejemplo, como los respaldos de disco a disco han mejorado sustancialmente el proceso tradicional de respaldo / recuperación.
2. La administración del ciclo de vida de la información a cambiado su dirección anterior orientada a mover la información a lo largo de diferentes niveles a almacenamiento, especialmente ejemplificada por el cambio hacia los modelos de replicación de datos en contraste con los de respaldo.
3. El cambio en los requerimientos de los negocios, que proveen nuevas políticas, procedimientos y prácticas.

La tecnología no es una situación ***deus ex machina.*** Los usuarios y sus ejecutivos deben poner en marcha las 4 P de la administración de procesos: política, procesos, procedimientos y prácticas. La tecnología habilita dichos componentes, pero no los remplaza.

- **Política**: define el curso de acción, no las acciones.
- **Procesos**: define las acciones a tomar para lograr los objetivos.
- **Procedimientos**: definen las acciones paso por paso, hacen que las políticas conduzcan a acciones.
- **Prácticas**: garantizan que los procedimientos que cumplen con las políticas sean llevados a cabo.

De esta manera, se debe comprender, primero que la información está en riesgo, tres ejes fundamentales:

a) Que se pierda como producto de eventos inesperados, físicos o lógicos que destruyan la información, lo que puede llevar a impactos severos sobre la operación o incluso al cierre definitivo de las operaciones.
b) Que sea robada, en otras palabras, obtenidos por terceros a la organización para propósitos distintos a los de la organización, especialmente el uso para fines delictivos o fraudulentos. No solamente esto puede afectar la salud financiera de los clientes de la empresa, sino que los daños mismos a la imagen corporativa, puede atentar contra la capacidad de la empresa de seguir haciendo negocios.
c) Que pierda validez o vigencia: problemas en la calidad de la información, así como la validez en el tiempo y su ciclo de vida, hace que la información, aunque se protegida y debidamente custodiada, resulte de poca utilidad para la organización. Si la información es incorrecta, deja de representar la realidad de los elementos claves del negocio, y si pierde su vigencia, elimina la capacidad de la organización de actuar en base a ella en el proceso de toma de decisiones y establecimiento de programas de acción.

Asocie la relación existente entre la protección de datos y la continuidad del negocio - 3p

La continuidad de negocio consiste en mitigar el riesgo causado por las interrupciones de las actividad y procesos normales de la empresa (Hill, 2009).

- Protege los intereses de los accionistas, la reputación de la marca, la buena voluntad de los clientes y a las actividades creadores de valor de la empresa.
- Los efectos del fallo de la continuidad de negocio oscilan entre: indeseables, inaceptables, severas hasta catastróficas.

La información almacenada de forma electrónica y la tecnología de información son solamente una parte del proceso general de continuidad de negocio, que involucra también al personal y activos no informáticos. La existencia, continuidad y bienestar del negocio están en un gran riesgo no mitigado si no existe un proceso formal que contemple la protección de los datos como parte del proceso de continuidad del negocio (Hill, 2009).

La información debe poder ser restaurada a un punto en que pueda trabajarse con ella: todo esfuerzo por remplazar o restaurar los equipos, redes o aplicaciones no cumplen ningún propósito si la información no puede ser restaurada en dicha condición.

La continuidad de negocio requiere de una superestructura de hardware y software sobre los sistemas claves de IT y as redes con los objetivos de (Hill, 2009):

- **Resistencia**: Lograr que las aplicaciones esenciales estén disponibles a todos sus usuarios todo el tiempo, a pesar de los fallos de los componentes individuales.
- **Alta disponibilidad**: que cuando los fallos no planeados conduzcan a que las aplicaciones esenciales no estén disponibles, estas se puedan recuperar en el menor tiempo posible, muchas veces medido en términos de algunos minutos por año.

Ilustre porque la típica tecnología de protección de datos todavía hoy en día deja mucho que desear – 3p

Hay que prestar atención a una serie cambios tecnológicos fundamentales (Hill, 2009):

- Arreglos redundantes de discos independientes (RAID, por sus siglas en inglés).
- El aumento en la capacidad de comunicación de grandes volúmenes de información a distancia.
- La aparición de los sistemas de respaldo disco-a-disco.
- La introducción de las tecnologías de respaldo basado en snapshots o respaldo continuo.

Estos cambios han cambiado las reglas de juego de los negocios tradicionales, que han llevado al nacimiento de las dinámicas de negocio 24x7, rompiendo con el paradigma día operativo / respaldo nocturno. Muchas de las prácticas relacionados con el procesos de protección y respaldo de los datos surgen en las organizaciones en momentos en la historia en la cual se podía esperar una dinámica de operación muy diferente a la recién descrita: durante el día de trabajo, digamos de 8 a.m. a 5 p.m., los sistemas información procesaban las operaciones del día, luego se suspendía el trabajo, se realizaban los respaldos en cinta magnética, poniendo en práctica técnicas de respaldo completos e incrementales y sistemas generacionales. Esto se archivaba para los respaldos operativos y eran enviados fuera de la compañía para manejar los esquemas de recuperación frente a desastres y/o se conservaban localmente para manejar los eventos operacionales.

No obstantes todos estos avances a nivel de la protección física, el cambio de los paradigmas de operación también trae a primer plano de criticidad la necesidad de mitigar los riesgos lógicos, cuya frecuencia e impacto se ven amplificadas dentro de este marco de operación continua.

Rara vez las empresas ponen en marcha un ambiente de mitigación de desastres multinivel, dónde uno cercano, mantiene la copia sincrónica (simultánea) de cantidades menores y más reciente o en tiempo real y uno más lejano, dónde se mantienen las copias de manera asincrónicas, a un menor costo y para volúmenes muchos más altos, con una menor frecuencia.

Finalmente, otra razón por la que los métodos de respaldo dejan mucho que desear es el costo mismo de la recuperación frente a desastres. Una vez realizadas las inversiones necesarias de recursos tecnológicas, humanos y de la tecnología de sincronización, en el caso de que el desastre se presente, el respaldo de la información ahora se encuentra solamente en los medios y / o sitio secundarios, lo que reduce la accesibilidad de la información.

Describa la relación entre el cumplimiento y la protección de datos – 3

El primer paso, es poseer una idea clara de que se entiendo por cumplimiento. Algunas definiciones (Hill, 2009):

- La respuesta compulsiva a un tercero autorizado, como el caso de un ente regulador gubernamental.
- Una respuesta voluntaria a una asociación de comercio o un cuerpo de una industria vertical con el propósito de adoptar prácticas comunes que faciliten la transacción a los clientes en oposición a utilizar una industria substituta.
- Una respuesta al mandato de un estándar industrial, por ejemplo, el PCI DSS[1].
- Una respuesta intencional e la empresa para protegerse de litigios.
- Una respuesta voluntaria para seguir buenas prácticas con tal de proteger propiedad intelectual, como patentes o secretos de negocio.

Una manera de simplificar la concepción del cumplimiento desde el punto de vista de protección de la información es dividiéndola en dos grandes áreas (Hill, 2009):

- **Lo que debe hacerse**
    - Preservar la información, saber cuál información se tiene, a dónde está y que las necesidades de reporte sobre dicha información pueden cumplirse dentro del plazo requerido.
    - La calidad de la información debe ir de la mano con la preservación de la información: muchos negocios suelen tener problemas en ponerse de acuerdo en la definición de entidades básicas de información, lo cual acrecienta las dificultades para manejar la consistencia.
    - La *auditabilidad* de la información es un nuevo objetivo de protección de la información.
- **Lo que no debe hacerse**
    - Leyes de protección de la privacidad suelen establecer de forma compulsiva como no puede ser utilizada la información provista por los clientes de la organización, con el propósito de llevar otros negocios.

[1] Payment Industry Data Security Standard.

Construya una tabla en la que resuma el rol de las personas, los procesos y la tecnología en el cumplimiento - 3p

PARTES	ROLES

PERSONAS	• Todos los trabajadores del conocimiento importantes deben estar envueltos:
	  ○ Personas internas con conocimiento y habilidades para lidiar con las leyes y las regulaciones.
	  ○ Personas de las áreas funcionales del negocio: son los interesados que, en el día a día, deben cumplir con las regulaciones
	  ○ Personas de la organización del Oficial de la Información en Jefe: especialistas en tecnología que aseguran que los sistemas de información y la información relacionada están funcionando y cumplen su propósito.
	• Una vez identificados los actores, el reto está en que cada uno aprendan sus partes y las ejecuten diariamente, esto normalmente está dirigido mediante procesos y habilitados por herramientas tecnológicas.

PROCESOS	• **Política**: define el curso de acción, no las acciones. • **Procesos**: define las acciones a tomar para lograr los objetivos. • **Procedimientos**: definen las acciones paso por paso, hacen que las políticas conduzcan a acciones. • **Prácticas**: garantizan que los procedimientos que cumplen con las políticas sean llevados a cabo.
TECNOLOGÍA	• Muchas veces los sistemas de información dan vida material a los procesos (instantiate), incluyendo los procesos de cumplimiento. En otras palabras, software que lleva a cabo los comportamientos de acuerdo con las políticas, sean estas adoptadas o compulsivas. • Software que facilitarla administración de los procesos de cumplimiento. La puesta en marcha de estos sistemas suelen ser una tarea que consume gran tiempo, y por lo tanto, una cantidad importante de recursos.

Explique porque el conocimiento de los datos es un objetivo de la protección de datos dentro de la gobernanza de los datos – 3

Se dice que se tiene conocimiento de los datos, en la medida que se cruza el punto entre conocer dónde se encuentra la información hacia información sobre el contenido mismo de la información, sus metadata. Por ejemplo, el conocimiento de los datos implica que una compañía pueda contestar a las siguientes preguntas:

- ¿Qué información tengo?
- ¿Cómo puede acceder a dicha información?
- ¿En qué formato está almacenada la información?
- ¿A que otros formatos puede la información ser convertidos de forma razonable?

La necesidad de dar respuestas a dichas preguntas, lleva a la conclusión de que hay que “levantar un inventario de datos” (Hill, 2009). Dicho inventario debe:

- Empezar con los servidores y subsistemas de almacenamiento administrados por TI.
- Incluir los lugares remotos, como las oficinas y sucursales.
- Cubrir a los equipos distribuidos, es decir, las estaciones de trabajo y dispositivos móviles, cómo laptops o teléfonos inteligentes.

De acuerdo con Loshin (2009) – Cap. 1 a 4

Explique lo que son datos maestros - 2p

Los datos maestros son los objetos centrales de negocio de la compañía, definidos, organizados y categorizados de forma consistente a partir de la información en sistemas transaccionales. Los datos maestros se alinean a grandes categorías, cada una de estas categorías definen a su vez las piezas de información o atributos de los datos maestros que deben estar correctamente registrados para poder entender al data maestro y su impacto en la empresa..

Los siguientes son ejemplos de datos maestros:

- Clientes.
- Empleados.
- Proveedores.
- Suplidores.
- Partes.
- Productos.
- Ubicaciones.
- Mecanismos de contacto.
- Perfiles.
- Contratos.
- Políticas.

Analice porque deben gestionarse – 2p

Los datos maestros deben gestionarse ya que, en un ambiente de información distribuida, la tendencia de la información a desorganizarse se ve magnificada. Los diferentes sistemas operaciones se construyen o se adquieren para atender necesidades específicas de departamentos o unidades de negocio, cada uno con diferentes ópticas y prácticas respecto al manejo de su información.

Dichos sistemas son mantenidos, administrados y utilizadas por diferentes grupos para tomar decisiones a su nivel, lo que no necesariamente está alineado con las perspectivas de las diferentes grupos de negocio o áreas funcionales de la organización.

Esto hace que sea bastante difícil los ejecutivos tener una visión integral de la organización, sus problemas, sus fortalezas. Es más, en muchos casos, líneas de negocio completas o personas individuales, pueden tener "intereses" incompatibles con el beneficio neto de una organización, por ejemplo, mantener negocios o clientes que en marco general de la compañía no son rentables o alineados con las fortalezas organizacionales.

De esta manera, el proceso de gestión de la información maestra, trae consigo la posibilidad de establecer un lenguaje común y de información de alta calidad, respecto a los elementos claves de la organización, detectar los problemas de calidad para concentrar debidamente los esfuerzos y, de forma más global, permitir la toma de decisiones basados en información y no en "intuiciones" del momento.

Resuma lo que impulsa la necesidad de tener datos maestros y su origen - 2p

Los elementos precursores de la necesidad de tener datos maestros es la aparición de la computación distribuida en la década de 1980 y el desarrollo en paralelo de la explosión de la computación de escritorio. Antes de esto, los equipos de una organización solamente disponían un solo recurso computacional, que albergaba todas las aplicaciones y sus conjuntos de datos (Loshin, 2009).

Debido a esta situación, dónde la información se encuentra distribuida, desagregada y en silos, la puesta en marcha de un plan de información maestra puede traer los siguientes beneficios (Loshin, 2009):

- Conocimiento comprensivo del cliente.
- Mejora en el servicio al cliente.
- Reportes consistentes.
- Mejora de la competitividad.
- Mejora en la administración del riesgo.
- Mejora en la eficiencia operativa y la reducción de costos.
- Mejora en la toma de decisiones.
- Mejor manejos de los costos de análisis y planeación.
- Cumplimiento de regulaciones.
- Aumento en la calidad de la información.
- Resultados más rápidos.
- Mejora en la productividad del negocio.
- Simplificación y consolidación de aplicaciones.

Construya una tabla en la que se indiquen las diferentes partes interesadas y una breve descripción de cada una – 2p

PARTES INTERESAS	DESCRIPCIÓN
ALTOS EJECUTIVOS	Ellos están interesados en demostrar que sus equipos han contribuido al desempeño de la organización. Les interesan que los procesos de información sean predecibles y que las nuevas iniciativas puedan ser desarrolladas. Tiene el interés de mantener a la organización comprometida y los procesos de datos maestro habilitan perspectivas de largo plazo en vez de programas tácticos de corto plazo, costos y difíciles de sostener en el tiempo.
CLIENTES COMERCIALES	Representan a las líneas de negocio para las cuáles, la disponibilidad de información de aplicación predecible y de alta disponibilidad representa el éxito de sus operaciones. Estos se benefician, especialmente por los impactos positivos de los procesos de calidad de la información, al ponerse en práctica los procesos de integración de la información.
DUEÑOS DE LAS APLICACIONES	Ellos en general, deben modificar sus procesos para ajustarse al uso de la información maestra en vez de sus copias locales. En particular, debe administrarse el riesgo potencial de la transición de un sistema probado (local) al sistemas no probado (información maestra).
ARQUITECTOS DE INFORMACIÓN	Debe colaborar para crear modelos que satisfagan las necesidades presentes y las futuras de la organización.
PRACTICANTES DE GOBERNAZA Y CALIDAD DE DATOS	Ellos son los responsables de introducir la propiedad, la guía y las herramientas de política para que los usuarios se ajusten a las nuevas restricciones a las formas de crear, acceder, usar, modificar y retirar la información.
ANALISTAS DE METADATOS	El proceso de datos maestros está altamente vincula con la disponibilidad y creación de los metadatos necesarios para crear los procesos.
DESARROLLADORES DE SISTEMAS	Las aplicaciones deben ser cambiadas, para acomodar los nuevos requisitos de movimiento de la información y retroalimentación de procesos de calidad. Así como los sistemas actuales, también los nuevos sistemas se desarrollaron sobre la premisa de que deben ser compatibles con la administración de datos maestros.
PERSONAL OPERATIVO	El personal operativo, muchas veces, para lograr que la tarea se ejecuten, han tenido que pasar por alto a los sistemas formales y a traer información a sus terminales locales, dónde terminan de procesarla de forma que pueda ser utilizada para cumplir con los negocios. De forma que sus hábitos deben cambiar para lograr que las entidades de información clave sean capturadas y migradas hacia el ambiente maestro.
(LOSHIN, 2009)	

Describa lo que es la gobernanza de los datos - 2p

El objetivo de la gobernanza de la información está circunscrito a asegurar que la información cumpla con las expectativas de todos los propósitos de negocio. Por lo tanto, debe evaluar y manejar los diferentes tipos de riesgos que subyacen dentro del portafolio de información empresarial.

Expresiones cualitativas respecto a la calidad de los valores individuales, los registros y la consistencia a través de múltiples elementos, representan el nivel más granular de la gobernanza de la información.

Cada elemento de datos debe tener un nombre, un formato estructural y una definición que debe ser registrado dentro de un repositorio de metadatos.

Dos técnicas son utilizadas principalmente para distribuir la gobernanza de la información a través de la empresa (Loshin, 2009):

1. Se define grupos de políticas de información, cada una de las cuales se imponen sobre el ciclo de vida de los elementos de información.
2. Se asignan protectores de la información, a los que se les asigna la responsabilidad de rendir cuentas, tanto por la calidad de los datos, así como por garantizar el seguimiento de las políticas.

Luego procede a definir conceptos, como entidades de información fundamentales, elementos de información críticos, políticas sobre la información, las métricas y la medición, monitoreo y evaluación.

Finalmente, se concentra en definir y proponer una estructura de rendición de cuentas y responsabilidad que permita garantizar que los dictados de la gobernanza de la información sean ejecutados. Dos son los factores fundamentales (Loshin, 2009):

1. Que exista una estructura administrativa que revise la ejecución.
2. Que el modelo de compensación recompense los comportamientos alineados con la gobernanza de la información.

Interprete lo que es la calidad de los datos y la gobernanza de los datos - 2p

La calidad de los datos es la evaluación de la propiedad de la información de describir la realidad histórica, y aún más importante, presente y futura de la organización. Incluye aspectos intrínsecos al dominio de datos, por ejemplo, las reglas de negocio y los metadatos, sin embargo, la calidad también involucra otras dimensiones como la eliminación de duplicaciones, así como los aspectos de validez de la información en el tiempo.

De esta manera, la calidad determina la capacidad de la información individual y agregada de aportar criterios para evaluar correctamente la realidad de la organización de moverse de un modelo de toma de decisiones intuitivas a uno amparada en datos concretos, comportamientos detectados y oportunidades medibles.

Por otra parte, la gobernanza de los datos es la estructura forma que existe en la organización para evaluar la calidad de los datos y establecer las acciones, deberes y responsables, de garantizar que se produzcan datos de calidad. No existen balas de plata de resuelvan los problemas de calidad. La gobernanza es el esfuerzo continuo, metódico, permanente y dirigido desde las más alta esferas de la organización, para que información de calidad sea producida en su lugar de origen, reducir o eliminar las redundancias y crear sistemas que unifiquen e integren la información a lo largo de la organización.

De acuerdo con Sarsfield (2009) – Capítulos del 1 al 3:

Explique cómo se define la gobernanza de los datos por sus beneficios - 4p

Sarsfield se enfoca en que a la hora de iniciar un proceso de gobernanza de la información debe definirse cómo se considera haber alcanzado él éxito.

Define entonces al éxito, como “la creación de una estructura organizaciones que supervise el uso corporativo de la información y haga mejor la vida de todos en la organización ” (Sarsfield, 2009).

Factores genéricos para el éxito de la gobernanza de la información:

- Corregir las anomalías de la información.
- Desarrollar un proceso repetible.
- Manejar el cambio.
- Coordinar el esfuerzo con el negocio.
- Establecer la propiedad de la información.

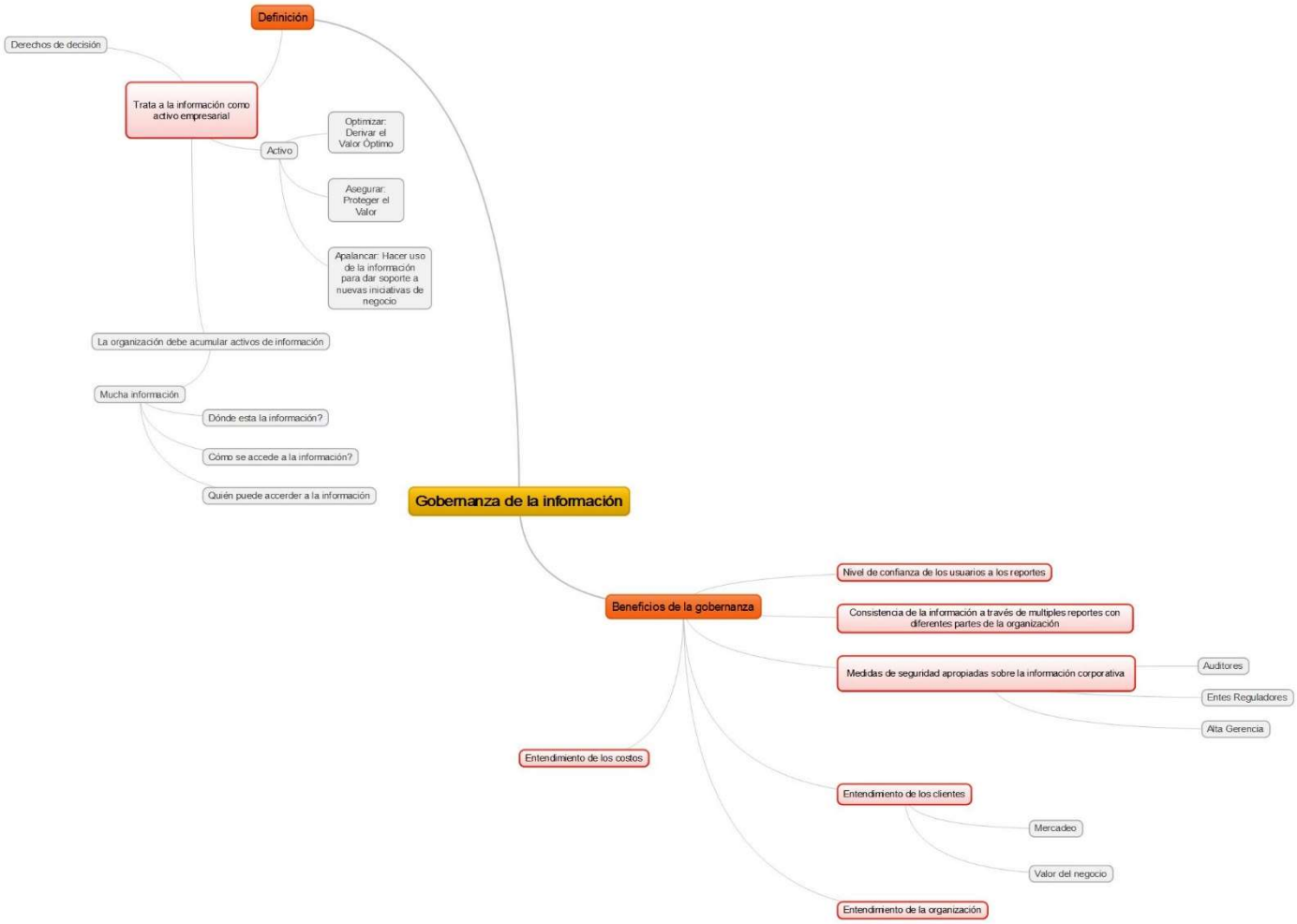
Describa cómo se define el éxito de la gobernanza de los datos - 4p

Diferentes actores, tienen diferentes perspectivas respecto a la gobernanza de la información:

- Los altos ejecutivos opinan que se trata de obtener eficiencia de parte de la organización, el mejor retorno de parte de los trabajadores del conocimiento y asegurarse que las personas cuentes con las mejores medidas para la toma de buenas decisiones.
- Para los usuarios de negocio, se trata de sus aplicaciones empresariales y de escritorio y de la información detrás de ellas.
- Para los tecnólogos, muchas veces se definen en términos del modelado de datos, que permitan establecer estándares sobre la información. Estos modelos son utilizados muy comúnmente en depósitos de datos y aplicaciones de inteligencia de negocios, así como en la administración de datos maestros.

De acuerdo con Solares (2010) – Capítulo 1:

Construya un mapa conceptual sobre lo que se indica en el capítulo de introducción a la gobernanza de los datos – 10p



De acuerdo con Fisher (2009) – Caps. 1 a 4:

Ilustre cómo lograr la transparencia con una fuerte gobernanza de los datos - 3p

La posición de Fisher respecto al logro de la transparencia basada en una fuerte gobernanza de datos se puede resumir de la siguiente manera: "*Regulaciones como la Sarbanes-Oxley (SOX) no dependen de listas de vigilancia, pero ciertamente requieren de datos precisos consistentes. Esta legislación establece los requisitos de gran transparencia en los sistemas de contabilidad y la revelación financiera. En particular, a incrementado el riesgo de los ejecutivos de las compañías que operan en bolsa, al imponer no solamente al riesgo de inversionistas furiosos sino también penalidades criminales. De tal manera, que los sistemas de contabilidad deben operar con la mejor información disponible*" (Fisher, 2009).

Para comprender bien el sentido, hay que entender el acercamiento de Fisher al planteamiento de la calidad de datos, que es una situación que se repite a lo largo de los 4 primeros capítulos, que son básicamente una arenga sobre los beneficios que los procesos de calidad pueden tener sobre los resultados económicos de la empresa.

- En el caso de las empresas públicas, que se cotizan en Bolsa, después del escándalo de ENRON, que reveló que una empresa que se presentaba como exitosa y boyante, era el resultado de una contabilidad creativa, y el vacío legal existente en los Estados Unidos para que los inversionistas pudieran perseguir penalmente a los ejecutivos responsables de propiciar dichos prácticas, se promulgo la legislación conocida como Sabanes-Oxley o SOX. En general, está normativa establece la responsabilidad de los ejecutivos de alto nivel de la compañía por velar que los procedimientos de control interno generalmente aceptados para el manejo contable y de los sistemas de información sean utilizados en la compañía. Desde el punto de vista de tecnología de información, esto ha llevado a la adopción de COBIT como marco de referencia.
- La falta de cumplimiento por los debidos procesos de control interno, implican la posibilidad de perseguir penalmente a los ejecutivos, por no velar por los controles internos generalmente aceptados.
- De esta manera el papel de la gobernanza de la información en estos casos no se basan en el uso de listas negras, dónde se establecen las personas o entidades sobre las que no se pueden hacer negocios, países sancionados y personas que tienen limitado la capacidad de realizar vuelos aéreos. En este caso, es más bien a través de procedimientos de transparentes de las operaciones financieras basados en prácticas generalmente aceptadas y que por lo tanto requieren restar respaldados por un fuerte proceso de calidad de datos, que muestre, de forma fehaciente la realidad de las operaciones económicas de la compañía así como las revelaciones importantes a los estados financieros. En una gran empresa, esto solamente es posible si se cuenta con procesos que aseguren una alta calidad y disponibilidad de la información, así como la detección temprana de problemas.

Explique cómo controlar los costos con datos precisos y fiables - 3p

El control de los costos con datos precisos y fiables es otro de los beneficios que Fisher describe que el gobierno de la información puede aportar a la organización, tanto es así que dedica la totalidad del capítulo tres a describirlo.

De la misma manera que los capítulos anteriores, es una exposición a los beneficios en lugar de un enfoque técnico de las maneras de lograrlo. No obstante, se pueden sacar las siguientes ideas principales. Hay al menos 7 actividades de control de costos que se ven beneficiados de información precisa y confiable:

- Modernización de la infraestructura de TI.
- Análisis de costos.
- Optimización de la cadena de suministros.
- Administración del inventario.
- Optimización del proceso de órdenes a efectivo.
- Reducción de los costos de mercadeo.
- Automatización de los procesos de negocios.

Es la posición de Fisher que: “las ganancias incrementales en la información sobre los costos producen grandes ahorros a la organización, sin la necesidad de incurrir en grandes gastos (Fisher, 2009)”. En otras palabras, el propone que hay que huir de la idea de grandes proyectos heroicos que pretenden resolver todos los problemas de calidad de una buena vez. Los mejores resultados se obtienen cuando se enfoca en un solo aspecto a la vez y se realizan mejoras sustanciales sobre dichos aspectos.

Bajo este esquema, la propuesta principal de parte es que, en un gran número de ocasiones, el efecto de los datos duplicados, son uno de las razones más importante por la cual la información no es útil, usando las 7 actividades anteriores, voy a plantear problemas de duplicación que pueden presentarse, que dificultan dichos objetivos:

- Duplicación de la información del cliente: muchos clientes están registrados más de una vez, con diferentes variaciones en el nombre, en el uso de los apellidos, en las contracciones de sus segundos nombres. Múltiples direcciones están asociadas a las múltiples instancias del cliente, en varios sistemas de registro. El medio por el cual el cliente contacta a la empresa, produce también duplicidad en las entradas de cliente. Las dos consecuencias fundamentales: a) se desconoce con precisión la información respecto al número de clientes; b) no se puede agrupar y establecer patrones de comportamiento del cliente. Los procesos de calidad permite mitigar y eliminar dicha duplicidad.
- Duplicación de la información de productos o insumos: la falta de estandarización en la información de productos, hace que poder responder preguntas de negocio como la utilización de las materias primas, así como el control de los gastos sea difícil. No se puede saber con certeza y precisión dónde se están produciendo dichos egresos. La gobernanza de esta información permite integrarla en registros maestros de productos. Esto posibilita el análisis de la información, toma decisiones, la detección de fugas, descubrir los patrones de consumo de la organización

Analice como se pueden lograr la optimización de ingresos con datos de calidad - 3p

Con el propósito de optimizar las utilidades es necesario conocer a los ciudadanos, los donadores o los clientes. Hay que saber que quieren y que no quieren. Todo está en los datos. La información impacta todos los aspectos la utilidad, incluyendo (Fisher, 2009):

- La lealtad de los clientes.
- La pérdida de los clientes.
- La adquisición de clientes.
- La ventaja competitiva.
- Reacción a los cambios del mercado.
- La innovación corporativa.

Los sistemas de CRM (Customer Relationship Management) se concentran en los árboles. Los programas de optimización de la utilidad se concentran en el bosque. Ambos requieren de información de alta calidad.

Las capacidades de calidad e integración de la información ayudan a las compañías a agregar la información, tomándolas de los sistemas de CRM y otros sistemas para crear un registro maestro de cada cliente. Al poseer un solo registro por cliente, en vez de múltiples versiones de la realidad se puede optimizar las estrategias para alcanzar a los clientes, mejorar la retención y maximizar los recursos.

Cuando la información de los clientes se encuentra dispersa entre múltiples sistemas de información, ese necesario algún tipo de puente entre los sistemas. De acuerdo a estudios, el 40% de las empresas inician proyectos de CRM u otro tipo sin evaluar los problemas de calidad de sistemas fuente. De la misma manera, el 2% de la información quede desactualizada mensualmente por los fenómenos de muerte, matrimonio o migración de los clientes (Fisher, 2009).

De esta manera, cuando se enfrenta a información de mala calidad, la optimización de la utilidad a través de un mejor conocimiento del cliente es muy difícil de lograr. De la misma manera, es muy difícil medir los resultados.

Una de las áreas más importantes dónde debe realizarse calidad de datos es en el proceso de eliminación de la duplicación (Fisher, 2009). En términos generales, es necesario utilizar procesos de calidad para eliminar la duplicidad a la hora de medir el número de cliente, sus direcciones de contacto, la duplicación producto de que el cliente llega a la compañía por múltiples medios. La eliminación de dicha duplicación permite racionalizar los recursos para diseñar campañas para alcanzar a los clientes, así como entender sus patrones de consumo.

De una forma simplificada, es posible optimizar los ingresos, conociendo los patrones de consumo del cliente y relacionándolos con los productos y los precios de la organización. Sin embargo, información precisa del comportamiento individual y de los resultados agregados es indispensable para lograr el objetivo. Las actividades de gobernanza de la información son las que logran que esta conocimiento puede ser generado.

De la caricatura que se utilizó para la actividad de la semana 3:

Construya una tabla en la que indique al menos 5 aspectos que van en contra de la seguridad y una medida de control que estime conveniente – 6p

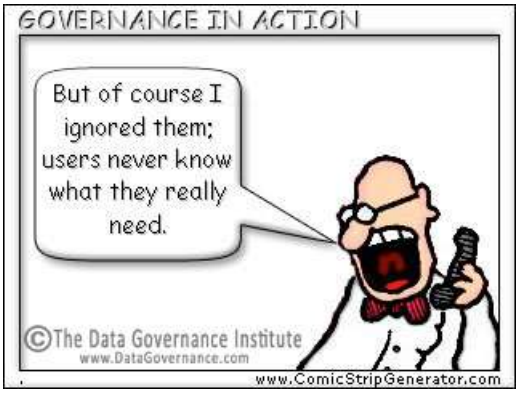
Aspectos que desfavorecen la seguridad	Medidas de control
Los nombres de usuario y contraseñas se encuentran a la vista, escritas sobre papel, el equivalente de dejar las llaves pegadas a la puerta. Utilización de contraseñas de baja seguridad, particularmente diminutivos del nombre: **toto, pepito**. De la misma forma, se comparten claves a través de líneas telefónica.	La puesta en marcha de una política integral de seguridad de las contraseñas junto al entrenamiento para su aplicación. Las políticas deben incluir requerimientos mínimos de complejidad, frecuencia de cambio de las contraseñas, la prohibición de compartir las mismas contraseñas, así como las políticas para su debido almacenamiento.
El manejo de las visitas de personas ajenas al departamento de tecnología de información especialmente visitantes externos no contemplan el acceso de estos a información sensitiva de la organización.	Procedimientos estandarizados para la atención de visitas externas, que incluyan recibirlos en lugar separados, así como el protocolo para manejarlos.
Las aplicaciones, como reportes gerenciales están abiertos en pantalla a pesar de que no hay nadie trabajando sobre ellos.	Debe establecerse políticas y entrenamiento sobre la necesidad de bloquear el equipo de cómputo cuando el operador se aleja de él. Dos medidas mínimas son necesarias: bloqueos cronometrados por falta de actividad, protocolos de acatamiento obligatorio sobre la necesidad de bloquear las terminales de trabajo cuando no son operadas.
Los dispositivos de almacenamiento extraíble, como unidades flash y diskettes están a la vista y alcance de la mano.	Los dispositivos extraíbles, en el caso de ser necesarios, deben almacenarse apropiadamente y solamente utilizarse en el momento en que se requieran hacen los movimientos de información, procediendo inmediatamente a ser guardados.
Dispositivos electrónicos y electromagnéticos como celulares y radios están adyacentes a los equipos informáticos.	Se debe establecer claramente áreas restringidas para colocar equipo electromagnéticos como celulares o radios. Dependiendo de las circunstancias y la información con la cúal se opera, puede ser necesario incluso prohibir su uso después de pasar la puerta.
La seguridad física de los sistemas de respaldo está comprometida, como muestra el caso de las tazas de café sobre las unidades de respaldo en cinta magnética.	No debe colocarse alimentos, y absolutamente prohibido bebidas, adyacentes a los equipos informáticos, especialmente aquellos relacionados con el almacenamiento de información.
Información sensible, como sueldos y presupuestos son manipuladas libremente y poseen etiquetas que claramente identifican la información, lo que la hacen fácilmente identificables como objetivos.	El manejo del etiqueta y transporte de la información sensible requiere de estrictos procedimientos de transporte y uso.
Los archiveros se encuentran abiertos y sin llave.	Los archiveros nunca deben dejarse abiertos y sin sus debidas llaves mientras no se estén introduciendo o sacando documento de ellos.
Documentos impresos descartados son descartados en el basurero normal sin los debidos procedimientos de destrucción.	Todo documento impreso que debe ser descartado en las áreas de procesamiento de la información debe ser un estricto proceso de destrucción, generalmente involucra la utilización de trituradores de papel y políticas sobre la disposición de dicho material una vez triturado.

De la caricatura que se utilizó para la actividad de la semana 4:

Construya una tabla en la que indique al menos 5 riesgos que atentan con la buena marcha organizacional y una medida de control que estime conveniente – 6pt

Riesgos de la buena marcha organizacional	Medidas de control
El uso incorrecto de las escaleras puede llevar a que se produzcan accidentes, particularmente acciones como: correr en las escaleras, el uso de lado incorrecto de la escalera para subir y bajar, transporte de objetos que obstaculicen la visibilidad al subir o bajar escaleras.	En términos generales. Aquí se trata de poner procesos de entrenamiento sobre la forma debida de utilizar las escaleras, en términos generales, dichos procedimientos deben ser visitados con al menos una frecuencia anual, bajo el modelo de cursos mandatorios.
El uso inapropiado de los dispositivos de limpieza puede producir accidentes con mucha frecuencia, en particular: de atender inmediatamente los derrames, dejar escobas o trapeadores apoyados contra puertas.	Deben establecerse proceso detallados sobre el manejo del equipo de limpieza y verificar que estos sean seguido de la forma como fueron diseñados.
Bloqueo de las rutas de evacuación con objetos que imposibilitan el paso.	Las rutas de evacuación deben mantenerse libre de bloqueo en todo momento y debe designarse personas directamente responsables de garantizar esta situación. Particularmente, el personal de seguridad es un buen punto de partida respecto a estos procedimientos.
Falta de atención (distracción) respecto al entorno hace posible la sustracción de oportunidad de suministros de oficina	El entrenamiento frecuente sobre los riesgos de robo o vandalismo es importante, ya que el nivel de alerta de las personas bajo cuando ha pasado un tiempo libre de eventos: realmente o porque no se ha percatado de que han sucedido.
Procedimientos incorrectos para agacharse a recoger objetos en el suelo puede producir accidentes.	En general, un entrenamiento programado sobre procedimientos de ergonomía y procedimientos para realizar estas tareas son vitales para prevenir estos riesgos.
Falta de uso de equipo de soporte lumbar cuando se manipulan cajas u otros objetos pesados.	En el caso de las personas que constantemente manipula objetos pesados, el uso mandatorio de equipo de soporte lumbar es necesario, para mitigar los riesgos de lesiones inducidas por este vector de riesgo.
Procedimientos inadecuados sobre la apertura y cierre de los archivos, particularmente, dejar abiertos archivos cuando no se están manipulando, es terreno fértil para accidentes o sustracciones de material sensible.	El desarrollo de costumbres y procedimientos adecuados sobre el manejo de los archivos es fundamental para prevenir estos riesgos. En particular, el entrenamiento sobre el debido protocolo sobre la utilización de los archivos debe ocurrir con la debida frecuencia.
Instalación incorrecta de las conexiones eléctricas puede llevar a electrocución.	En este caso, el seguir protocolos previamente establecidos respecto a la disposición de equipos de conexión eléctrica, incluyendo la posición de las regletas y otras fuentes es crucial. En la medida de los posible, en un ambiente cubicular, la instalación eléctrica debe estar a la altura de las manos de un escritorio, en general a un metro de altura. Debe evitarse las instalaciones eléctricas que corren por el suele, y en el caso de ser estas estrictamente necesarias, debe estar apoyadas directamente contra las paredes.
Manipulación incorrecta de los alimentos, dentro o fuera de lugares designados para esta operación, fácilmente puede producir accidentes como derrames y manchas que pueden dañar equipo, así como producir accidentes humanos.	Deben acondicionarse apropiadamente los sitios designados para el consumo de alimentos, así como la ubicación estratégica de los equipos eléctricos como hornos, hornos de microondas y refrigeradoras. En particular, no deben ser ubicado más allá de la altura de los brazos extendidos de una persona de altura media.

Ingrese en el sitio http://www.datagovernance.com/ busque el apartado de "Data Cartoons", seleccione una caricatura, analícela e interprete su significado - 6pt



Esta caricatura tiene un alto nivel de resonancia de mi parte. Existe una tendencia, especialmente de parte de la gente de tecnología de información, de muchas veces desarrollar sus soluciones en una proverbial "torre de marfil", sin presentar la debida atención a las necesidades concretas que los usuarios les están emitiendo.

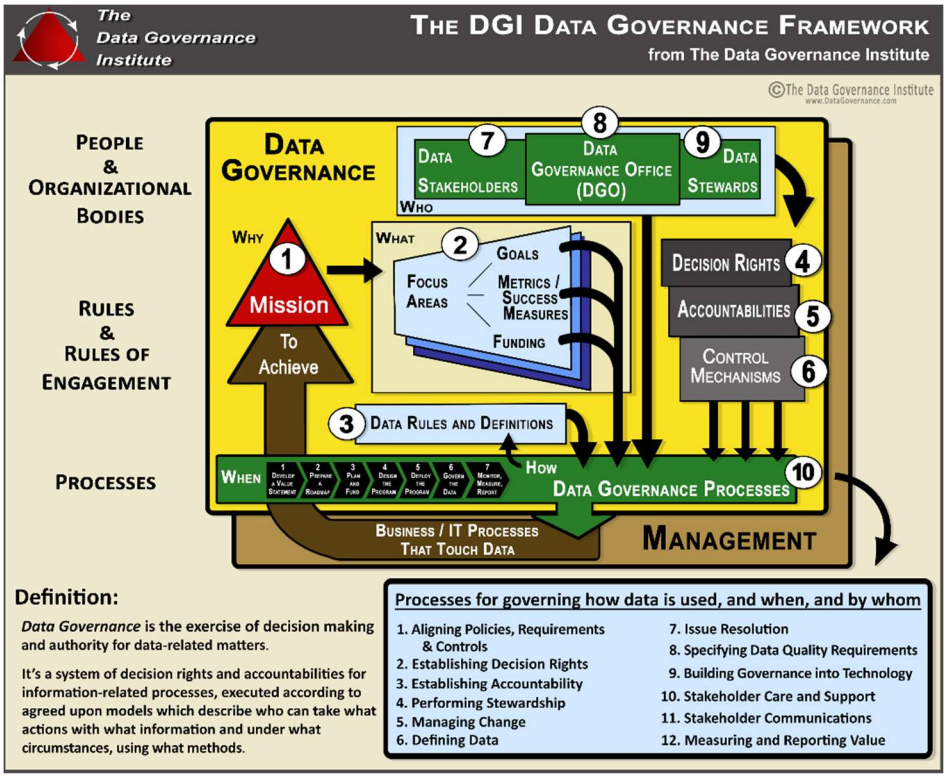
Ciertamente, para muchos usuarios no informáticos, existen dificultades para expresar sus necesidades en términos tecnológicos, digamos, como tablas, llaves, índices, formularios de entrada, etc. Por lo mismo, es importante que la gente de tecnología de información, en el momento de atender las necesidades de los usuarios, se "desconecte" temporalmente del mundo de la programación y los sistemas y se ponga el "cassette" del administrador de negocios. En este caso, es importante entender la tarea, el objetivo de negocio, la información requerida, las transformaciones sobre los datos, los métodos de toma de decisión de parte del operador, en fin, las necesidades del cliente.

Muchas veces esto significa que en el proceso de gobernanza de la información se designe persona en medio del proceso, que tenga un pie en cada mundo, uno en la comprensión de las necesidades del negocio y el otro en los detalles del mundo de los sistemas de información, para poder trasladar los requerimientos de negocio en requerimientos de sistemas, así como coordinar apropiadamente la comunicación entre los departamentos.

De la misma manera, más allá de establecer los canales de comunicación apropiadas, está el factor de que debidamente se esté prestando atención a las necesidades expresadas por los clientes en los sistemas de información con los que trabajan a diario.

Con este propósito, muchas veces es importante desarrollar técnicas apropiadas para confirmar que lo que la persona está recibiendo como requerimientos, expresen adecuadamente las necesidades de los clientes. El uso de interfaces simuladas, la participación del cliente durante las fases iniciales del proceso de desarrollo de las aplicaciones, es crítico también.

Ingrese en el sitio http://www.datagovernance.com/ busque el apartado de "The DGI Framework", luego "The DGI Data Governance Framework", ubique la imagen con el marco de referencia, analícelo, interprételo y haga una explicación del mismo - 10pt



El marco de referencia del DGI, debe entenderse como un flujo que va desde y hacia los procesos de gobernanza de la información, de esta forma, los procesos de gobernanza son un buen punto de partida, ya que designa lo que espera que ocurra al ponerse en práctica la gobernanza de la información:

De esta manera, el HUB de procesos identifica 7 procesos de gobernanza de la información:

1. Desarrollar una declaración de valor.
2. Preparar un mapa de ruta.
3. Planear y obtener los fondos.
4. Diseñar el programa.
5. Poner en marcha el programa.
6. Gobernar la información.
7. Monitorear, mediar, reportear.

Una vez establecidas estas tareas que ocurren en el programa de gobernanza de la información, se puede visitar el flujo de alimentación del programa:

1. **Misión**, el porqué: debe establecerse una misión clara de por qué se está poniendo en marcha el programa. Esta misión debe ser comprensiva y no limitarse a uno o más objetivos de calidad de la información, sino más bien a los impactos concretos que se espera obtener con la puesta en marcha del programa. De esta forma, podemos ver cómo la gran flecha café apunta que los 7 pasos del HUB de procesos, tienen como propósito último, alcanzar la misión del programa.
2. **Áreas de enfoque**, el qué: una vez establecida la misión, se establecen las áreas de enfoque, que definen de forma concreta que resultados se esperan, como se van a medir estos resultados, cómo se considera que se ha alcanzado el éxito en este proceso. De la misma manera, el establecimiento adecuado de lo que se quiere lograr es el punto de partida para establecer cuanto va a costar esto y por lo tanto, obtener el financiamiento apropiado.
3. **Reglas de información y definiciones**: se trata de un proceso interactivo entro los 7 procesos de gobernanza de la información y las definiciones de lo que se considera una data de alta calidad y fiabilidad. Esto trata desde los elementos de bajo nivel, como la definición de los tipos de datos, las restricciones de contenido, el universo de los datos, el establecimiento de definiciones globales que pueden ser comprendidas por la totalidad de la organización, así como el caso particular de procesos especiales, la definiciónes especiales que pueden tenerse sobre ciertos tipos de información.
4. **Derechos de decisión**: quién puede tomar cuáles decisiones y bajo que circunstancias.
5. **Rendimiento de cuentas**: quién debe presentar los resultados obtenidos por las diferentes tareas del proceso.
6. **Mecanismos de control**: que actividades y puntos de control son necesarios para darles seguimiento a los responsables de rendir cuentas y tomar decisiones, de que están ocurriendo bajo los procedimientos correctos y por las personas debidamente designadas.
7. **Las partes interesadas**: una clara definición de las personas y organizaciones que están interesadas en los resultados del proceso de gobernanza, lo que esperan en forma particular de él y el efecto que estas expectativas tiene sobre los responsables de la información.
8. **La Oficina de Gobernanza de la Información**: en este modelo, se estable la necesidad de establecer un órgano centralizado responsable de dar seguimiento al programa de gobernanza de la información. Esto es de especial importancia ya que estos programas deben coordinar los esfuerzos de las unidades de negocio y las personas responsables de la calidad de los datos individuales, junto a los esfuerzos tecnológicos para recopilar estos datos, diagnosticar sus problemas y evaluarlos, que en muchas ocasiones, implica asegurarse que las soluciones tecnológicas son puesta en marcha y que se supervisen sus resultados.
9. **Las personas responsables de la información (stewards)**: esto definen las personas responsables de la calidad de la información individual. Es un área extensa ya que en la mayoría de las ocasiones, involucra a las personas que están realizando la introducción inicial de la información así como los

programas que interactúan de frente con los clientes, proveedores y otros interesados, para garantizar que la información se esté recopilando de forma correcta.

Bibliografía

Berson, A., & Dubov, L. (2007). *Master data management and customer data integration for a global enterprise* (2 ed.). United States: McGraw-Hill.

Ed Gelbstein, P. (2012). Strengthening Information Security Governance. *ISACA Journal*, 1-6.

Fisher, T. (2009). *The Data Asset - How Smart Companies Govern Their Data for Business Success.* Hoboken: Wiley Sas.

Hill, D. G. (2009). *Data Protection - Governance, Risk Management and Compliance.* Boca Raton, Florida, United States: Auerbach Publications.

Loshin, D. (2009). *Master Data Management* (1 ed.). Elsevier, Massachussets, United States: Morgan Kaufmann Publishers.

Sarsfield, S. (2009). *The Data Governance Imperative : A business strategy for corporate data.* Cambridgeshire: IT Governance Publishing.

Solares, S. (2010). *The IBM Data Governance Process : Driving Business Value with IBM Software and Best Practices.* MC Press Online, LLC.