POLÍTICAS Y BUENAS PRACTICAS DE GOBIERNO DE DATOS EN EL DESARROLLO DE PROYECTOS DE INTELIGENCIA DE NEGOCIOS (BI).

JUAN DAVID CARDONA PÉREZ

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA "UNAD"
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA, COLOMBIA
2021

POLITICAS Y BUENAS PRACTICAS DE GOBIERNO DE DATOS EN EL DESARROLLO DE PROYECTOS DE INTELIGENCIA DE NEGOCIOS (BI).

JUAN DAVID CARDONA PÉREZ

Proyecto de Grado para optar al título de:
Especialista en Seguridad Informática

Directora de Proyecto
Ingeniera Yenny Stella Núñez Álvarez

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA "UNAD"
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA, COLOMBIA
2021

TABLA DE CONTENIDO

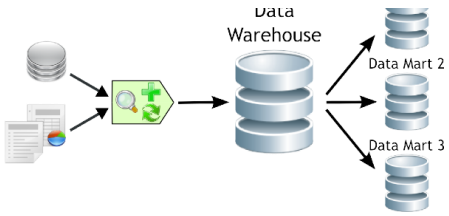
Resumen

La presente monografía tiene como objeto definir las políticas y buenas prácticas para el buen gobierno de los datos almacenados en medios informáticos, los datos pueden estar en un sistema de gestión de base datos, ya sea de manera local, remota o en la nube, en archivos fuentes, como planos o archivos Excel, en gestores Big Data o base de datos Non SQL; se define el alcance del gobierno de datos en los desarrollo de Inteligencia de Negocios (En adelante: BI), estos desarrollos tienen como objetivo darle valor a los datos, por lo tanto la información, aun en ambiente de desarrollo, se presenta de forma completa y verdadera, siendo esto un punto crítico de seguridad de información, la empresa debe salvaguardar, la información de terceros y la de la propia empresa.

Para obtener el resultado esperado se realizará la consulta sobre las políticas generales y los controles definidos en el estándar NTC ISO/IEC 27001/2013 y aquellas que complementen, modifiquen o sustituyan esta norma, así mismo se definirá las buenas prácticas de un Sistema de Gestión de Seguridad de la Información (SGSI) definiendo una estrategia de gestión de los datos basada en los criterios de la información (Confidencialidad, integridad y disponibilidad)criterios básicos para el desarrollo de soluciones BI.

Lo anterior con el fin de dar el tratamiento adecuado a los datos que sean facilitados al equipo de desarrollo, datos que a su vez son incorporados en base de datos, data warehouse[1], datamarts[2] e incluso sistemas de alojamiento en la nube o sistemas distribuidos tanto internos como externos a la compañía a la cual se está desarrollando el proyecto.
Para entender mejor estos conceptos lo ilustraremos de forma gráfica

Imagen 1 Data warehouse y data mart



Fuente: Webyempresas. [sitio web]. Data warehouse y data mart . [Consulta: 23 de septiembre de 2019]. Disponible en : https://www.webyempresas.com/que-es-un-data-mart/

Palabras clave: Keywords. datawerehouse, datamarts, Business intelligence, ISO 27001, ISO 27003.

---

[1] Fuente: Webyempresas. [sitio web]. Data warehouse y data mart . [Consulta: 23 de septiembre de 2019]. Disponible en : https://www.webyempresas.com/que-es-un-data-mart/
[2] Ibid..

Abstract

The purpose of this monograph is to define the policies and good practices for the good governance of data stored in computer media, the data can be in a database management system, either locally, remotely or in the cloud, in source files, such as plans or Excel files, in Big Data managers or Non SQL database; The scope of data governance is defined in the development of Business Intelligence (Hereinafter: BI), these developments are intended to give value to the data, therefore the information, even in a development environment, is presented in full and true, being this a critical point of information security, the company must safeguard the information of third parties and that of the company itself.

In order to obtain the expected result, the general policies and controls defined in the NTC ISO / IEC 27001/2013 standard and those that complement, modify or replace this standard will be consulted, as well as the good practices of a Management System Information Security (ISMS) defining a data management strategy based on the information criteria (Confidentiality, integrity and availability) basic criteria for the development of BI solutions.

The foregoing in order to give the appropriate treatment to the data that is provided to the development team, data that in turn are incorporated into database, data warehouse3, datamarts4 and even cloud hosting systems or distributed systems both internal and external to the company to which the project is being developed.

To better understand these concepts, we will illustrate it graphically

Fuente: Webyempresas. [sitio web]. Data warehouse y data mart . [Consulta: 23 de septiembre de 2019]. Disponible en : https://www.webyempresas.com/que-es-un-data-mart/

Keywords. datawerehouse, datamarts, Business intelligence, ISO 27001, ISO 27003.

[3] Ibid...,
[4] Ibid…,

INTRODUCCIÓN

En la actualidad cualquier sector empresarial apoya sus procesos sobre las Tecnologías de la Información y las comunicaciones (En adelante: TIC), estas se han convertido en un elemento primordial en el incremento de la competitividad de las empresas. Las TIC permiten mejorar la calidad de los servicios y generar beneficios a las empresas que las implementan y administran de manera adecuada.

El concepto clave para maximizar los beneficios que se pueden obtener de las TIC, es el concepto de Gobierno de TI, este concepto agrupa los procedimientos estratégicos que facilitan a la empresa analizar y tomar decisiones en el área tecnológica.

De igual forma, las empresas actuales, manejan un alto flujo de información, algo que era inimaginable; contar con un mundo en el que la masividad de la información en ocasiones se hace insostenible. Es así como gracias a esa cantidad de datos la empresa de hoy cuenta con mayores instrumentos de análisis y recolección de estos.

Se ha sostenido que el conocimiento es poder, y en la actualidad el conocimiento es generado por el procesamiento de la información, en tal sentido las empresas intentan transformarse y las grandes multinacionales fortalecerse, para ello han iniciado el uso de herramientas de acople y análisis de información masiva de datos, siendo una de las más mencionadas últimamente en el área de TI “Business Intelligence”. Haciendo referencia aquella herramienta que puede ayudar a las empresas a adquirir un mejor entendimiento en su interior dependiendo el Core de su negocio y en general de ellas mismas.

Lo anterior gracias a la capacidad de explotar su información, con la intención de poder manipular los datos adquiridos de una manera más sencilla, y así entender el porqué de su desempeño o, mejor aún, plantear escenarios a futuro, lo cual ayudará a tomar mejores decisiones, corrigiendo las acciones presentes y previendo las futuras (acciones decisorias prospectivas). Sin embargo, estos datos siempre estarán expuestos a terceros por cuanto las empresas de desarrollo de soluciones de inteligencia de negocios, al igual que aquellas que desarrollan software a la medida. Por otro lado, la implementación tanto de herramientas como de protocolos que garanticen la seguridad de la información es de vital importancia y necesidad. Por consiguiente, ya no basta con implementar proyectos de inteligencia de negocios porque es la moda, sino que se hace imperativo el diseño de una guía que sintetice y guíe hacia las buenas prácticas y la implementación de metodologías de seguridad en el desarrollo que faciliten la creación de información de valor de manera confiable y acorde con las exigencias del mercado, teniendo como valor agregado el componente de seguridad en cada fase del proceso.

Es así como para el diseño de la presente guía de buenas prácticas, se realizó primero, la recolección de las mejores prácticas de seguridad y de gobierno TI propuestas por los estándares ISO internacionales, posteriormente se clasificaron y midieron estas prácticas asociando factores de riesgo en la implementación de los proyectos informáticos consolidando el desarrollo de este trabajo de investigación en un documento guía.

Como resultado se tiene la guía de buenas prácticas de seguridad para el desarrollo de soluciones de inteligencia de negocios con base en una metodología de desarrollo seguro como lo es PSP/TSP[5], enmarcado bajo estándares internacionales de seguridad como lo sugiere la norma ISO 27001 y con la estandarización de los procesos descritos por las prácticas que implementa el nivel 2 de madurez de CMMI[6] en las empresas de desarrollo de soluciones informáticas.

Imagen 2 MODELO CMMI

Fuente: Tutorialspoint. [Sitio web]. SEI CMMI - Niveles de Madurez. [Consulta: 04 de agosto de 2019]. Disponible en:https://www.tutorialspoint.com/es/cmmi/cmmi_maturity_levels.htm

[5] Tutorialspoint. [Sitio web]. SEI CMMI - Niveles de Madurez. [Consulta: 04 de agosto de 2019]. Disponible en:https://www.tutorialspoint.com/es/cmmi/cmmi_maturity_levels.htm
[6] Ibid.,

1. PLANTEAMIENTO DEL PROBLEMA

El acceso a la tecnología informática en la última década se ha convertido en un insumo accesible en costos y de gran importancia para las empresas, encontrando en la informática un aliado en la gestión y resolución de problemas, con un alto índice de asertividad, lo cual se logra mediante la implementación de la inteligencia de negocios, estos factores hacen que el dato o el conjunto de datos y metadatos tenga un valor cuantificable para la empresa o el dueño de estos, pero estos datos se ven expuestos y vulnerados si no se garantiza de manera eficiente y eficaz la protección de los mismos.

De acuerdo con la investigación establecida por el Doctor Andrés Ricardo Almanza Junco, se identifica cuatro incidentes principales en los sistemas informáticos, el primer incidente se relaciona con la instalación de software no autorizado con el (55,56%), En segundo lugar, se identifica los Virus/Caballos de Troya (46,3%), el tercer incidente acceso no autorizados a la web. En consecuencia, la fuga de información sigue en la escala de lo identificado (19,14%), lo que muestra el panorama actual de los peligros existentes. A nivel Nacional la tendencia en incidentes se mantiene en Colombia.

Si se tiene en cuenta que los anteriores incidentes son reportados por empresas donde su principal activo de información son los datos por la gran cantidad de información que recibe, almacena, analiza y procesa con base en un sofisticado gobierno de datos como es el caso de Walmart. Quien con más de 245 millones de clientes que visitan 10.900 tiendas y con presencia en 10 países en todo el mundo, Walmart es definitivamente una de las tiendas retail más importantes. Este gigante estadounidense recopila 2,5 petabytes de datos no estructurados cada hora de un total de 1 millón de clientes. Para que podamos hacernos una idea, 1 petabyte equivale a 20 millones de archivos. Con esta inmensa cantidad de información que genera la compañía cada hora, Walmart[7] necesita mejorar su eficiencia operativa mediante el aprovisionamiento de una importante infraestructura de Big Data. Con ello, es una de las compañías que mejor ha sabido extraer valor de los datos.

Con base en la gran cantidad de transacciones de datos que se realizan diariamente y en la forma como se estructuran los mismos generando información accionable dentro de un proyecto de inteligencia de negocio, por cuanto se hace necesario el diseño e implementación de una guía de políticas y buenas prácticas de gobierno de datos en el desarrollo de proyectos de inteligencia de negocios (BI).

[7] Projectpro. [Sitio web]. Análisis de Big Data. [Consulta: 30 de septiembre de 2020]. Disponible en : http://www.dezyre.com/article/how-big-data-analysis-helped-increase-walmart-s-sales-turnover/109

El panorama Regional frente a estos incidentes lo revela la firma ESET que en su informe de 2018 ESET SECURITY REPORT [8], preciso los datos estadísticos frente a los incidentes informáticos en la región, allí se evidencio que los países donde las empresas sufren mayor vulnerabilidad se encuentran en su orden, Perú con un 25% México con un 20% y Argentina con un 14%.

No obstante que a nivel nacional Colombia se encuentra en quinto lugar con un 10% superado por Brasil con un 14% el país sigue estando en deuda frente a un estudio detallado, acerca de las vulnerabilidades y reporte de incidentes en cada uno de los sectores, tal como lo evidencio desde el año 2016, el ministerio de las telecomunicaciones y la OEA que desde 2016 informo acerca del estudio.

"con la participación de 18 representantes de **Asobancaria, la Andi, el Departamento Nacional de Planeación y los Ministerios de Educación, Justicia, Relaciones Exteriores y Defensa, además de delegados de la Policía Nacional, el Ejército y la Fuerza Aérea,** para iniciar el primer estudio sobre el impacto económico de los incidentes, amenazas y ataques cibernéticos en Colombia"[9].

[8] Welivesecurity. Informe de 2018 Eset Security Report Latinoamerica 2018. [Recuperado el 11 de noviembre de 2019] Disponible en: https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

[9] Mintic. [Consulta: 13 de octubre de 2019]. MinTIC y OEA iniciaron estudio del impacto de incidentes cibernéticos en Colombia. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/16129:MinTIC-y-OEA-iniciaron-estudio-del-impacto-de-incidentes-ciberneticos-en-Colombia

2. FORMULACIÓN DEL PROBLEMA.

¿Cómo diseñar la guía de políticas y buenas prácticas para el gobierno y gestión de los datos empresariales en el desarrollo e implementación de proyectos de inteligencia de negocios (BI)?

3. JUSTIFICACIÓN.

Teniendo como base la forma como las TIC han revolucionado el mundo y con ellas las nuevas formas de negocio, mayormente basadas en la manera como las empresas gestionan y procesan sus datos, previo a su almacenamiento e identificación, los mismos se han convertido en su mayor activo, toda vez que la reunión de miles de estos datos producen información invaluable para la toma de decisiones estratégicas de las compañías, es por ello que aparece el gobierno de datos, representado en la gestión de la disponibilidad, integridad, usabilidad, confidencialidad y seguridad de los datos utilizados en una empresa, principios y características que debe de tener la información de acuerdo a los estándares internacionales ISO 27001 y a los sistemas de gestión de seguridad de la información (SGSI).

La implementación de un gobierno de datos se debe realizar cuando la gestión tradicional de los datos implementada ya no es suficiente y no ofrece la seguridad e integridad requerida en el dato transformado en información, cuando se tienen millones de registros diarios la gestión de dato se convierte en una tarea exclusiva de un departamento de la empresa, la cual realiza el análisis, control y seguimiento a las políticas de gobierno de datos, en este sentido el manejo tradicional del dato se vuelve insuficiente, se necesitan niveles de seguridad del datos ya sea por cumplimiento de normas generales o compromisos contractuales que exigen un manejo de los datos más formal.

El gobierno de datos debe estar alineado en virtud de la Ley Estatutaria 1581 de 2012, constituida como el marco general de la protección de datos personales en Colombia y la norma técnica ISO/IEC 27001.

Las políticas de datos logran mecanismo para lograr que las entidades eleven su nivel de seguridad y calidad.

El gobierno de datos es quien pone las reglas sobre la gestión de la información. Esta diferencia entre el gobierno y la gestión de datos se ha convertido en un tema clave en la toma de decisiones empresariales.

Philip Russom, Director de Investigación para Data Management en TDWI, propone siete razones que justifican el gobierno de datos[10]:

[10] SAS. [Sitio web]. 7 razones por las cuales la Gestión de datos necesita del Gobierno de datos. [Consulta: 13 de noviembre de 2019]. Disponible en: https://blogs.sas.com/content/sasla/2014/05/28/7-razones-por-las-cuales-la-gestion-de-datos-necesita-del-gobierno-de-datos/

- ✓ La gestión de datos necesita el ambiente colaborativo que provee el gobierno de datos.
- ✓ La gestión de datos necesita de las capacidades de administración del gobierno de datos.
- ✓ La gestión de datos necesita de los procesos del gobierno de datos para la gestión del cambio.
- ✓ La gestión de datos necesita del mandato del gobierno de datos.
- ✓ La gestión de datos necesita del gobierno de datos para incrementar el alcance dentro de la empresa.
- ✓ La gestión de datos necesita la guía del gobierno de datos a medida que madura a nuevas generaciones.
- ✓ La gestión de datos necesita que el gobierno de datos soporte sus prioridades.

Además de las razones expuestas por Phillip, la puesta en marcha de una guía de políticas y buenas prácticas de gobierno de datos en el desarrollo de proyectos de inteligencia de negocios (BI)., servirá como documento de apoyo a las facultades de ingeniería, economía, administración y todas aquellas áreas del conocimiento anexas que dentro de sus objetivos se encuentre el procesamiento y la gestión de datos, personales y /o empresariales.

De igual forma servirá como guía de referencia para las empresas que desee implementar un sistema BI o aquellas que teniéndolo no garantiza las características de la información.

4. OBJETIVOS.

4.1. OBJETIVO GENERAL.

Construir guía de políticas y buenas prácticas para el Gobierno de Datos en el desarrollo de proyectos de Inteligencia de Negocios BI.

4.2. OBJETIVOS ESPECIFICOS.

- Analizar los lineamientos de las normas NTC ISO/IEC 27001, 27002, 27003 asociados a la gestión de los datos informáticos y la Ley Estatutaria 1581 de 2012 de Colombia conocida como Ley Habeas Data.

- Identificar los riesgos y vulnerabilidades en el desarrollo de los proyectos Inteligencia de Negocios BI utilizando la metodología MAGERIT V3.

- Cuantificar los riesgos y vulnerabilidades utilizando la metodología MAGERIT V3 en las dimensiones de disponibilidad, integridad y confidencialidad. tomando como fundamento la norma técnica NTC ISO/IEC 27001 anexo A.

- Construir guía de políticas y buenas prácticas para al desarrollo de proyectos de inteligencia de negocios BI. Tomando como fundamento la norma NTC ISO/IEC 27001 y 27002.

5. MARCO REFERENCIAL.

5.1. ESTADO DEL ARTE.

La palabra “Datos” proviene del latín “Datum”, que significa “lo que se da”, el dato por sí solo no representa o aporta ninguna información, un número es simplemente un número, pero, si a este número se le asocia un documento como lo puede ser un pasaporte, registro civil o de nacimiento, el simple número se convierte en información, que sumado al factor tiempo genera valor estadístico.

En los sistemas informáticos empresariales los datos son recibidos en conjunto, transformándose en información empresarial y esta información es manipulada para generar valor a la empresa y se desarrollen soluciones administrativas u operativas en torno a la información procesada.

Sobre este hecho la información pasa a ser indudablemente el activo más importante con que cuenta la empresa. De tal forma que, un mal manejo de la información puede afectar el valor final generado, por lo anterior, nace el Gobierno de TI y en unos de sus lineamientos, el Gobierno de Datos, este gobierno garantiza la integridad y seguridad de la información, sin un gobierno de datos establecido, la información empresarial no puede ser gestionada efectivamente, propendiendo con ello a la fuga de información, adulteración de la información, información imprecisa o en el caso más grave su perdida.

El gobierno de datos debe regirse sobre políticas o guías de buenas prácticas, en tal sentido se toma como marco de referencia las normas ISO, normas internacionales ampliamente difundidas y aceptadas en el ámbito empresarial e incluso judicial.

En la actualidad para el manejo de grandes volúmenes de datos se tienen técnicas de Big Data o la transformación de la información para generar valor con la ciencia de datos y la BI, estas técnicas generan indicadores, donde se puede conocer el funcionamiento táctico y estratégico de la empresa en una sola visualización y en tiempo real.

Nos encontramos fren a un tema en el cual hay muy poca literatura, el desarrollo de aplicaciones de BI se puede asociar con los desarrollos de programas y a gobierno de datos, estos últimos temas si cuenta con una bibliografía más amplia para su estudio y comprensión.

5.1.1 MADUREZ GOBIERNO DE DATOS.

José Jaime Garcés Zuluaga de la Universidad Pontificia Bolivariana[11], en su trabajo de grado nos da a conocer la caracterización al menos cuatro modelos de madurez de gobierno de datos, mediante una recopilación bibliográfica y análisis, con el fin de dar criterios a las organizaciones en la selección del modelo de madurez más adecuado y que mejor se adapte a su situación. Se presenta como guía para todas aquellas empresas que estén interesadas en implementar un correcto gobierno de dato.

5.1.2 GOBIERNO DE DATOS, UN POTENCIADOR DE LOS SISTEMAS DE GESTIÓN DE CALIDAD.

Juan Darío Portilla Romero[12], en su artículo nos describe como la gestión de los datos es una herramienta eficaz para el desarrollo empresarial y gestión de las organizaciones. La gestión de datos es una herramienta eficaz para el desarrollo de los componentes de un sistema de gestión en las organizaciones.

Anteriormente se pensaba que el gran problema radicaba en el salvaguardo de los datos, pero este concepto se ido formando en el sentido que los datos poseen un ciclo de vida, desde que nacen hasta que se guardan y es de importancia tener el control en cada una de las fases donde se realiza cualquier gestión sobre el dato.

5.1.3 DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMATICA.

Andrés Palacios Ortega de la Universidad Libre[13] realiza la investigación sobre como diseñar las políticas en cuanto al gobierno de datos en una entidad pública nacional, donde se parte desde el primer problema el cual es la anticuada tecnología que se posee en ciertas dependencias del estado.

---

[11] GARCÉS ZULUAGA, José Jaime . Caracterización de Modelos de Madurez en gobierno de datos. [En línea]. Trabajo de grado para Magister en TIC. Universidad Pontificia Bolivariana, 2016. [Consultado el 22 de agosto de 2019]. Disponible en: https://repository.upb.edu.co/bitstream/handle/20.500.11912/2583/INFORME_FINAL_%20Jose%CC%81%20Jaime%20Garce%CC%81s.pdf?sequence=1&isAllowed=y

[12] PORTILLA ROMERO, Juan Darío. Gobierno de datos, un potenciador de los sistemas de gestión de calidad. [En línea]. [Consultado el 06 de julio de 2019]. SSN: 2145-1389 / Vol. 9 / N.º 2 / 2017 / pp. 159-172. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6726297.pdf

[13] PALACIOS ORTEGA, Andrés. Diseño de un modelo de políticas de seguridad informática para la Superintendencia de Industria y Comercio de Bogotá.[En línea]. Proyecto de grado para e ingeniero de sistemas. Universidad Libre de Colombia , 2015. [Consultado 18 de septiembre de 2019]. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/8926/PROYECTO_DE_GRADO_ANDRES_PALACIOS.pdf?sequence=1

5.2 MARCO CONTEXTUAL.

En la actualidad, el Gobierno de Datos ha ido aumentado su importancia dentro de la pequeña y mediana empresa, esto se debe al crecimiento de la información que se recibe y almacena, con este crecimiento se incrementan los problemas en la gestión de la información, conllevando a que los controles comunes en ocasiones sean insuficientes ante la alta demanda de registros, por lo anterior el Gobierno de Datos se ha transformado en una de las principales prioridades estratégicas para las empresa, en un buen gobierno, reside el control, la seguridad, la disponibilidad e integridad de la información.

El Gobierno de Datos tiene como objetivo la gestión de información registrada en los medios informáticos con la finalidad de cumplir los objetivos empresariales y representa la unión de la calidad de datos, gestión, políticas, gestión de procesos de negocio y gestión de riesgos, que comprende el tratamiento de los datos de una organización.

Ahora bien, aunado a la información se encuentra las técnicas de Inteligencia de Negocios, un informe de Gartner corrobora que el sector de analítica de datos y BI alcanzará un volumen de negocio mundial cercano a los 18.300 millones de dólares, y en tres años será de 22.800 dólares (+25%).

Igualmente, las previsiones sugieren que la inteligencia de negocios aumentará **en tres años en un 25%**, debido a que estos sistemas darán **accesibilidad, agilidad y conocimiento para dar continuidad a los negocios.**[14]

El informe Gartner establece lo siguiente para el año 2020:

- El 50% de las consultas analíticas se generarán a través de búsqueda, procesamiento de lenguaje natural o voz, o se generarán automáticamente.
- Las organizaciones que ofrecen a los usuarios acceso a un catálogo de datos internos y externos obtendrán el doble de valor empresarial de las inversiones analíticas que las que no lo hacen.
- El número de expertos en análisis y datos en unidades de negocios crecerá a una tasa tres veces mayor que la de los expertos en departamentos de TI, lo que obligará a las empresas a repensar sus modelos organizativos y sus habilidades.

5.3 MARCO TEÓRICO.

[14] Thinkbig .[Sitio web]. El Business Intelligence será una tecnología fundamental en el crecimiento de los mercados. [Consulta:12 de mayo de 2019]. Disponible en: https://blogthinkbig.com/el-business-intelligence-sera-una-tecnologia-fundamental-en-el-crecimiento-de-los-mercados

5.3.1 Gobierno de Datos.

Imagen 3 Gobierno de Datos

Fuente: Cobit 4.1 del IT Governance Institute 2008

Se puede definir el Gobierno de Datos, como la disciplina encargada de articular personas, procesos y tecnología, permitiendo a la empresa apalancar la información como un recurso de valor empresarial, y al mismo tiempo, es el encargado de mantener a los usuarios, auditores y reguladores satisfechos, usando la mejora de la calidad de los datos garantizando la permanencia de los clientes, generando nuevas oportunidades en el mercado.

IBM plantea los siguientes seis pasos para un buen gobierno de datos[15]

- Establecer metas. Sentencias principales que guían la operación y desarrollo de la cadena de suministro de información.
- Definir métricas. Conjunto de medidas usadas para evaluar la efectividad del programa y los procesos de gobierno asociados.
- Tomar decisiones. La estructura organizacional y el modelo de cambio ideológico para analizar y crear políticas de decisión.
- Comunicar políticas. Herramientas, habilidades y técnicas usadas para comunicar decisiones políticas a la organización.
- Medir resultados. Comparar resultados de las políticas con las metas, entradas, modelos de decisión y comunicación para proveer constante retroalimentación sobre la efectividad de la política.
- Auditar. Herramienta usada para comprobar todo.

[15] IBM.[Sitio web]. Seis pasos para el Gobierno de Datos. [Consulta: 09 de junio de 2019]. Disponible en: https://www.ibm.com/developerworks/ssa/data/library/techarticle/gobierno-datos/index.html

En Colombia la tendencia a implementar proyectos BI va en aumento constante, las empresas cada vez más fijan sus objetivos en el cuidado, seguridad y disponibilidad de su información; pero no tienen en cuenta que, sin el adecuado manejo y aseguramiento de esta, la empresa perderá privilegios frente a otras perdiendo competitividad.
De acuerdo con el estudio global "Anlytics como fuente de innovación empresarial", realizado por el Instituto Tecnológico de Massachusetts en 2017, más de la mitad de las empresas en el mundo (55 %), usan los datos como herramienta de conocimiento e influencia para obtener ventajas competitivas en el mercado y para planificar sus estrategias comerciales.[16]
De igual manera las plataformas de análisis de información y predicción actualmente constituyen una fuente clave para las empresas que las incorporan en sus aplicaciones, en este sentido es imperativo que dentro del gobierno de datos y en el desarrollo e implementación de estas soluciones se cuente con una guía de buenas prácticas.

Ahora bien, revisemos los principios que rigen el gobierno de datos.

5.3.2 Principios del gobierno de datos.

1. Garantizar la integración de datos: y también de metadatos (de negocio, técnicos y de operaciones).
2. Cubrir el ciclo de vida del dato al completo: tener visibilidad sobre su origen, los caminos que ha seguido y su destino es la misión de la aplicación de este principio del gobierno de datos.
3. Velar por la seguridad del dato: así como de todo lo que tiene que ver con su privacidad y confidencialidad.
4. Asegurar la calidad de los datos: definiendo, controlando y mejorando los procesos.
5. Conocer el linaje del dato: a través del aseguramiento de la trazabilidad de las aplicaciones.
6. Apoyar la misión de gobierno de datos: aportando eficacia a los procesos de gestión de datos y uso de estos.
7. Establecer reglas aplicables a los datos fuera de las bases de datos: para convertir en útil toda la información que se contiene en documentos externos a los sistemas, pero que también se considera de valor.
8. Determinar todo lo relativo a la función de data storage: concretando qué datos son susceptibles de ser almacenados, en qué volumen y cuál será su ubicación.

[16] Portafolio. [Sitio web]. Así le va a las empresas en Colombia que usan tecnología de análisis de datos. [Consulta: 23 de abril de 2019]. Disponible en: https://www.portafolio.co/negocios/empresas/empresas-en-colombia-que-usan-tecnologia-de-analisis-de-datos-512836

5.3.3 Inteligencia de Negocios (BI)

¿Qué es Inteligencia de Negocios?

El termino Business Intelligence (BI) fue creado en 1958 por H. P. Luhn su papper "A Business Intelligence System" de IBM Research "Se refiere a las tecnologías, aplicaciones y prácticas para la recolección, integración, análisis y presentación de la información empresarial y a veces también a la información en sí misma."

Inteligencia de Negocios, por sus siglas en ingles de Business Intelligence BI, según el Data Warehouse Institute, lo define como la combinación de tecnología, herramientas y procesos que me permiten transformar mis datos almacenados en información, esta información en conocimiento y este conocimiento dirigido a un plan o una estrategia comercial[17].

Business Intelligence (BI) o inteligencia de negocios se define como la habilidad corporativa para tomar decisiones. Esto se logra mediante el uso de metodologías, aplicaciones y tecnologías que permiten reunir, depurar, transformar datos, y aplicar en ellos técnicas analíticas de extracción de conocimiento . BI se puede definir como el uso de los datos recopilados con el fin de generar mejores decisiones de negocio, esto implica accesibilidad, análisis y revelar nuevas oportunidades.

BI es el conjunto de metodologías, aplicaciones y tecnologías que permiten reunir, depurar y transformar datos de los sistemas transaccionales e información desestructurada en información estructurada, para su explotación directa o para su análisis y conversión en conocimiento, dando así soporte a la toma de decisiones sobre el negocio.

5.3.4 Ciclo de vida desarrollo BI.

El ciclo de vida de un desarrollo refiere a los siguientes pasos:

1. **Etapa de Extracción (ETL):** Por sus siglas en inglés, Extract, Transform, Load; Extracción, Transformación, Carga. El proceso de desarrollo de un proyecto de inteligencia de negocios en una empresa debe iniciar en la identificación de las fuentes de información, estas fuentes puedes estar dispersas en la empresa y pueden estar en diferentes archivos (Excel, Planos) y en diferentes base de datos relaciones y NoSQL, el proceso ETL permite realizar la extracción, transformarla y cargar en una sola fuente de datos a la se llama Data Warehouse o Data Smart, en este proceso se debe asegurar la integridad, coherencia y disponibilidad en el destino.

[17] Oracle. [Sitio web]. ¿Qué es Inteligencia de Negocios?.[Consulta: 04 de abril de 2019]. Disponible en : https://www.oracle.com/ocom/groups/public/@otn/documents/webcontent/317529_esa.pdf

2. **Etapa de Consolidación:** Consiste en el proceso automático de recopilación de las diferentes fuentes con el fin de normalizar, depurar y estructurar la información, una vez finalizado estos procesos se procede a la carga de los datos en la bodega de datos corporativa.

3. **Etapa de Explotación**: Consiste en la aplicación de las herramientas existentes para dejar listos los datos sobre la bodega corporativa, se da acceso a los usuarios que estén en capacidad de aprovechar y explotar la información ya depurada y filtrada, sobre esta etapa se tienen dos tecnologías que nos permiten realizar el proceso de explotación.

   La primera son los cubos OLAP, por sus siglas en inglés, (On-Line Analytical Processing). cuyo objetivo es agilizar la consulta de grandes cantidades de datos.

   La segunda es la minería de datos que consiste en la aplicación de un conjunto de métodos, para el procesamiento y análisis de datos, se basa en los conceptos de "escarbar y explotar". Así, grandes volúmenes de datos son tratados mediante diversos procesos para permitir el descubrimiento de información no evidente, elementos de utilidad y comportamientos interesantes como: cambios, anomalías, estructuras significativas y patrones de comportamiento para aplicarlos a nuevos conjuntos de datos.

4. **Etapa de Visualización**: Consiste en mostrar a los usuarios la información gestionada en herramientas "Reporting", se visualizan como tableros de mando Dashboard o como Balance Scored Card, en reportes dinámicos o datos exportados a tablas de cálculo como lo es Microsoft Excel.

5.3.5 Sistema de Gestión.

Es el encargado de la implementación de los procesos que ayudan a que una organización ejecute servicios o productos de forma confiable y acorde a las especificaciones internacionales.

El Sistema de Gestión de Seguridad de la Información, según **ISO 27001** consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización[18].

[18] PMG. [sitio web]. ¿Qué es un SGSI?. [Consulta: 13 de marzo de 2019]. Disponible en : https://www.pmg-ssi.com/2015/07/que-es-sgsi/

5.3.6 Análisis de riegos.

El análisis de riesgo da un panorama a la empresa sobre que se enfrenta, cuáles son sus vulnerabilidades y cuáles son los niveles críticos tolerados, para realizar este análisis se adopta la metodología MAGERIT, que es una metodología de análisis y gestión de riesgos de los sistemas de información, y se apoya con PILAR, que es un procedimiento informático - lógico para el análisis y gestión de riegos, que sigue la metodología MAGERIT.

5.3.7 Seguridad informática.

Para esto se toma como norma la NTC-27001 como modelo, la cual puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande.

5.3.8 Norma ISO

ISO son las siglas en inglés International Organization for Standardization. Se trata de la Organización Internacional de Normalización, y se dedica a la creación de estándares para asegurar la calidad, seguridad y eficiencia de productos y servicios. Son las llamadas Normas ISO[19].

5.3.9 Norma ISO 27000

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

Las normas ISO 27000 tienen una similitud con las normas de Gestión de Calidad ISO 9000, son una serie de estándares con un rango que va de la 27000 a 27019 y de 27030 a 27044. Cada una de las normas de la familia 27000, establece todos los aspectos prácticos de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, tanto en públicas y privadas.

[19] Certificadoiso9001. [Sitio web]. ¿Qué es ISO? [Consulta: 14 de abril de 2019]. Disponible en: https://www.certificadoiso9001.com/que-es-iso/

5.3.10 Seguridad de la Información

La información es un activo de valor para las empresas; representa un conjunto de datos los cuales, de acuerdo con la misión de la empresa, estos deben ser protegidos de acuerdo a las leyes naciones, esta información vuelve competitiva a la empresa, a esto los datos deben estar protegidos ante fuga de información o manipulación o mal uso de estos.

El resultado del crecimiento tecnológico, la exposición de la información es mayor ampliando las amenazas y las vulnerabilidades. La información está contenida en muchos medios:

- Impresa.
- Almacenada en soporte informático (cinta, discos, memorias).
- Grabaciones en video y voz.

Las amenazas sobre la información son de tres tipos, internas, externas y/o naturales, que se definen de la siguiente forma:

Externas: Acceso no permitido en las redes y medios informáticos de la empresa y/o acceso no autorizado a las instalaciones físicas, los accesos pueden ser, por ejemplo: spam, hackers, suplantación de identidad, fraude, espionaje, sabotaje, robo de información, entre otras.

Internas: Las cuales se generan al interior de la empresa, principalmente por el conocimiento del personal vinculado directa o indirectamente a la empresa. Los ejemplos sobre estas amenazas pueden ser: alteración de la información, divulgación de la información, fraudes, robo, sabotaje, uso no autorizados de sistemas informáticos, uso de imagen corporativa sin autorización, entre otras.

Naturales: Las generadas por desastres naturales, como inundaciones, huracanes, terremotos, incendios, entre otras.

5.3.11 Ciclo de Vida del Dato.

El modelamiento del ciclo de vida del dato se concentra en garantizar desde la obtención hasta la eliminación el dato, existen varias metodologías para aplicar el ciclo de vida del dato, las cuales son:

- DAMA
- POSMAD
- COBIT

La metodología DAMA, nos enseña que el dato se adquiere, se almacena o se mantiene, se usan y finalmente se destruyen, el ciclo de vida según DAMA es el siguiente:

- Planificar.
- Especificar.
- Habilitar.
- Crear y adquirir.
- Mantener y usar.
- Archivar y recuperar.
- Eliminar.

La metodología PSOMAD, que consiste en las siguientes actividades procedimentales:

- Planificar.
- Obtener.
- Almacenar y compartir.
- Mantener.
- Aplicar.
- Eliminar.

La metodología COBIT, nos propone un ciclo de vida para el dato, entre los procesos de gobierno y gestión, estos procesos son:

- Planificar.
- Diseñar.
- Construir y adquirir.
- Usar y/o operar, que contiene los procesos de almacenar, compartir y usar.
- Monitorizar, que comprende los procesos de monitorizar y mantener.
- Desechar, que se compone de archivar o destruir.

5.3.12 Gobierno Vs Gestión del Dato.

La palara “gobierno” se ha generalizado y puesto de moda. En Otto (2013) se recopila la relación que existe entre Gobierno de Datos, Gestión de Datos y Gestión de Calidad del Dato, por lo anterior podemos definir:

- **Gobierno de datos** cuyo objetivo principal es que el dato alance el valor óptimo maximizando el beneficio de la actividad empresarial.

- **Gestión de datos** debe proporcionar los mecanismos e insumos tecnológicos necesarios y suficientes para poder satisfacer los requisitos para asegurar la adecuación de los datos, implantando los mecanismos de monitoreo del nivel de calidad de datos.

- **Gestión calidad de datos** tiene que proporcionar los requerimientos de calidad de datos en la capa de gestión de datos, adicional debe adecuar los procedimientos necesarios para el monitoreo de la gestión de calidad.

Dentro de las normas de la familia ISO/IEC 38500, es sin duda las más importante para el Gobierno de las TSI, se encuentran dos normas relacionadas con el gobierno y gestión de los datos.

- ISO/IEC 38505-1, Governence of IT – Part I: The application of ISO/IEC 38500 to the governence of data , en el que se aplica el modelo de la ISO/IEC 38500 al Gobierno de datos.

- ISO/IEC 38505-2, Governence of IT – Part 2: The application of ISO/IEC 38500-1 for data magnament , que controla la gestión de dato de la norma anterior.

5.3.13 Metodologías para la gestión de riesgos.

La gestión de riesgos son los procesos de identificación, análisis, tratamiento y monitoreo de los riesgos que debe realizarse en toda empresa, en este caso particular, en dos tiempos, en la empresa de desarrollo de las soluciones de datos y la empresa donde se implementa el desarrollo, con el fin de compilar su probabilidad de ocurrencia y el impacto que generaría en la integridad y disponibilidad de los datos Existen varias metodologías y normas que ofrecen una lista de procedimientos para la correcta implementación de la gestión de riesgos en una organización, a continuación, se describen 3 de ellas, más para el presente monografía fue elegida la metodología MAGERIT como referencia:

5.3.13.1 NTC ISO 31000.

Brinda los principios y las procediditos estándar en la gestión del riesgo. Esta metodología puede ser utilizada por cualquier tipo de empresa y no es específica para ninguna industria o sector, adicional se puede aplicar en toda la organización y a un amplio rango de actividades que va desde las estrategias hasta productos, servicios y activos. Además, se puede aplicar a cualquier tipo de riesgo, cualquiera sea su naturaleza, bien sea que tenga consecuencias positivas o negativas. Según

ISO 31000 los principios que debe cumplir toda organización que desee aplicar una correcta gestión del riesgo son:

- La gestión del riesgo crea y protege el valor.
- La gestión del riesgo es una parte integral de todos los procesos de la organización.
- La gestión del riesgo es parte de la toma de decisiones.
- La gestión del riesgo aborda explícitamente la incertidumbre.
- La gestión del riesgo es sistemática, estructurada y oportuna.
- La gestión del riesgo se basa en la mejor información.
- La gestión del riesgo está adaptada.
- La gestión del riesgo toma en consideración los factores humanos y culturales.
- La gestión del riesgo es transparente e inclusiva.
- La gestión del riesgo es dinámica, reiterativa y receptiva al cambio.
- La gestión del riesgo facilita la mejora continua de la organización.

5.3.13.2 MAGERIT.

Responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos de ISO 31000.

Magerit propone dos grandes tareas a realizar:

1. Análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar.

2. Tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

5.3.13.3 NIST SP 800-30.

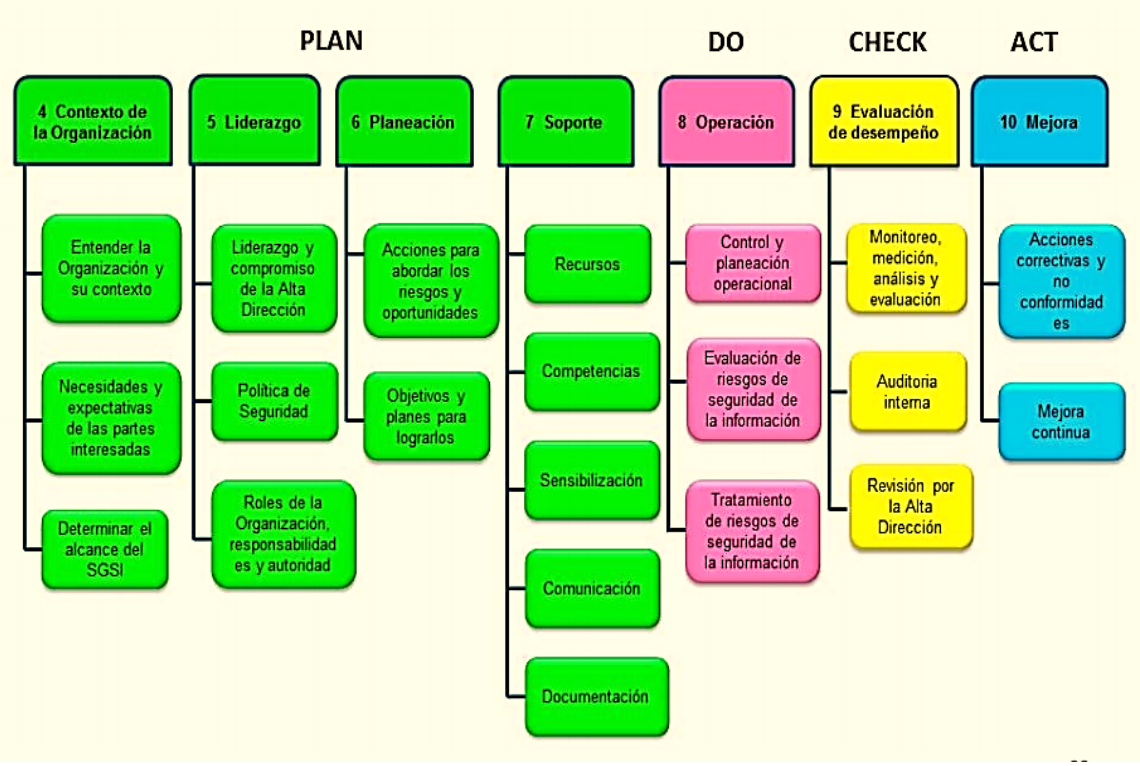
NIST SP 800-30 Proporciona una base para el desarrollo de un programa eficaz de gestión de riesgos, que contiene tanto las definiciones y la orientación práctica necesaria para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI.

La gestión del riesgo puede estar dirigida a los tres niveles de la jerarquía de gestión

del riesgo (Organización, Procesos de misión o negocio y sistemas de información) siendo la valoración del riesgo un componente clave en el proceso de gestión de riesgo que se realiza a nivel holístico en una organización. Dicho proceso de gestión de riesgo incluye: Demarcar los riesgos, evaluar los riesgos, responder a los riesgos y monitorear los riesgos (NIST SPECIAL PUBLICATION 800-30, 2012)

5.3.14 Requisitos de la Norma ISO 27001.

Imagen 4 Requisitos de la Norma ISO 27001



Fuente: Certificadoiso9001. [Sitio web]. ¿Qué es ISO? [Consulta: 14 de abril de 2019]. Disponible en: https://www.certificadoiso9001.com/que-es-iso/

5.3.14.1 Contexto de la Organización.

Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.

5.3.14.2 Liderazgo.

Requisitos específicos para la alta dirección.

5.3.14.3 Planificación.

En este punto se abordan los problemas, riesgos y oportunidades y se fijan los objetivos y planes de la seguridad de información.

5.3.14.4 Soporte.

En este punto se inicia con un requerimiento que las organizaciones deben determinar y proveer los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el SGSI. Expresado de forma simple, este es un requerimiento muy poderoso que cubre todas las necesidades de recursos de un SGSI.

Finalmente, existen requerimientos para 'información documentada'. Estos requerimientos están relacionados con la creación y actualización de información documentada y su control.

5.3.14.5 Operación.

Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.

5.3.14.6 Evaluación del Desempeño.

En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado.

5.3.14.7 Mejora.

Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una, no, conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

5.4 MARCO CONCEPTUAL.

Confidencialidad: Hablamos de confidencialidad cuando no referimos a la característica que asegura que los usuarios sean (personas, procesos, etc.), no tengan acceso a los datos a menos que estén autorizados para ello.

Disponibilidad: Garantiza que los recursos de sistema y la información estén disponibles solo para usuarios autorizados en el momento en que los soliciten.

Integridad: Nos indica que toda modificación de la información solo es realizada por usuarios autorizados, por medio de procesos también autorizados.

ISO: International Standards Organization. Una de las organizaciones de normalización más importantes. El gobierno de cada país está representado individualmente. (Diaz, Mur, San Cristobal, Castro, & Peire, 2012)

Gobierno de datos: La gobernabilidad de los datos consiste en la gestión de éstos, en pro de los objetivos empresariales, y representa una convergencia de la calidad de datos, gestión, políticas, gestión de procesos de negocio y gestión de riesgos, que comprende el tratamiento de los datos de una organización.

BI: Siglas del inglés Bussiness Intelligence, inteligencia de Negocios

5.5 MARCO LEGAL.

Ley Estatutaria 15 81 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales

Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

NTC 27001:2013: Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información. Requisitos.

NTC 27002:2013: Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.

ISO/IEC TR 18044:2004: Ofrece asesoramiento y orientación sobre la seguridad de la información de gestión de incidencias para los administradores de seguridad de la información y de los administradores de sistemas de información.

Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

6. METODOLOGIA DEL DESARROLLO.

6.1. TECNICAS DE RECOLECCION DE DATOS

El proceso de recopilación de información es uno de los puntos cruciales en el desarrollo del proyecto, básicamente se fundamenta en el análisis y síntesis de las buenas prácticas de desarrollo seguro de software identificadas en los estándares y metodologías seleccionados para el estudio (norma ISO 27001, ISO 27002 y MAGERIT v3), cada una de estas normas y metodología respectivamente cuenta con su documento oficial y puntos guía que describe y desarrollo cada una de las normas y metodología.

6.2. TECNICAS DE PROCESAMIENTO DE DATOS

La metodología utilizada para la recopilación de las vulnerabilidades en el desarrollo de soluciones BI es la MAGERIT, con esta metodología se realza el procesamiento de datos utilizado los dominios de la ISO 27002 obteniendo los indicadores que facilitan el proceso de categorización de las mejores prácticas de desarrollo seguro de soluciones BI bajo los estándares de la ISO 27001.

6.3. ALCANCE DEL PROYECTO.

El tratamiento de los datos siempre ha de ser de especial atención para los usuarios finales como en el desarrollo de las aplicaciones informáticos empresariales, por tal motivo la presente monografía tiene como alcance el análisis y evaluación de riesgos de la seguridad de información en el área de gobierno de datos para el proceso de desarrollo de soluciones de inteligencia de negocios BI, dando como resultado final la construcción de la guía de políticas y buenas prácticas en el tratamiento de la información en el desarrollo de soluciones BI.

6.4. FASES DEL DESARROLLO

El proyecto se desarrolla en tres FASES:

1. **Documentación y análisis**: En esta fase se realiza la identificación de las vulnerabilidades en cada uno de los dominios seleccionados, que permitan evaluar efectivamente los impactos de seguridad en el desarrollo de soluciones BI descritas por las normas ISO 27001 y 27002.

2. **Evaluación y selección**: Con las vulnerabilidades identificadas se especifican los controles de acuerdo al conjunto de prácticas seguras para el desarrollo de soluciones BI, se caracterizan cuales vulnerabilidades poseen mayor impacto y cuales deben tener mayor control.
3. **Guía de buenas prácticas**: Se realiza el documento final de guía de buenas prácticas de acuerdo a los resultados e indicadores obtenidos en la evolución de las vulnerabilidades y especificación de los riesgos y la identificación de los posibles factores de riesgo que pudieses derivarse de la implementación.

7. DESARROLLO DEL PROYECTO.

A continuación, se realiza la identificación, análisis y evaluación de los activos y riesgos de seguridad de la información en el proceso de desarrollo de soluciones de Inteligencia de Negocios BI.

7.1. NOMENCLATURA DEL DESARROLLO.

La metodología con la cual se va a desarrollo el proyecto es la MAGERIT V3, esta metodología tiene su nomenclatura especial la cual se describe a continuación

Tabla 1 Nomenclatura Activos

Activos
[D] DATOS
[K] CLAVES CRIPTOGRAFICAS
[S] SERVICIOS
[SW] SOFTWARE
[HW] EQUIPAMENTO INFORMÁTICO
[COM] REDES DE COMUNICACIONES
[Media] SOPORTE DE INFORMACIÓN
[AUX] EQUIPAMENTO AUXILIAR
[L] INSTALACIONES
[P] PERSONAL

Fuente: ENS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. [Recuperado el 23 de junio de 2018]. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

Tabla 2 Dimensiones MAGERIT

Dimensiones	
[D]	Disponibilidad
[I]	Integridad
[C]	Confidencialidad
[A]	Accesibilidad
[T]	Trazabilidad

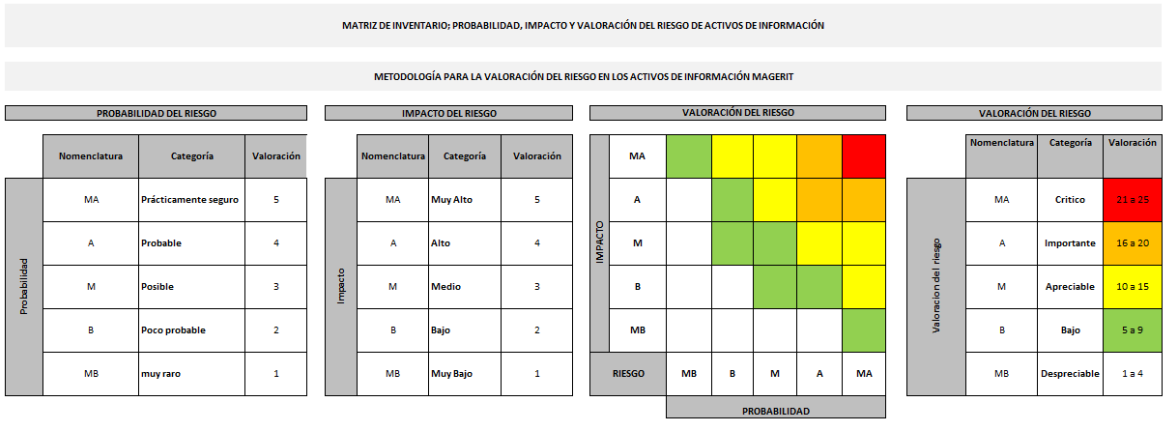
Fuente: ENS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. [Recuperado el 23 de junio de 2018]. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

Tabla 3 Criterio de Valoración

Criterios de Valoración		
VALOR		CRITERIO
25	MA	Daño extremadamente grave
20	A	Daño muy grave
15	M	Daño grave
9	B	Daño importante
4	MB	Daño menor

Fuente: Autor

Tabla 4 Calificación MAGERIT



MATRIZ DE INVENTARIO; PROBABILIDAD, IMPACTO Y VALORACIÓN DEL RIESGO DE ACTIVOS DE INFORMACIÓN

METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN MAGERIT

PROBABILIDAD DEL RIESGO

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

VALORACIÓN DEL RIESGO

IMPACTO						
	MA					
	A					
	M					
	B					
	MB					
RIESGO		MB	B	M	A	MA
		PROBABILIDAD				

VALORACIÓN DEL RIESGO

	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: ENS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. [Recuperado el 23 de junio de 2018]. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

7.2. IDENTITICAR ACTIVOS.

El primer paso en la metodología MAGERIT es la identificación de los activos que van intervenir, en este caso concreto, en el desarrollo de la solución de BI.

Tabla 5 Identificar Activos

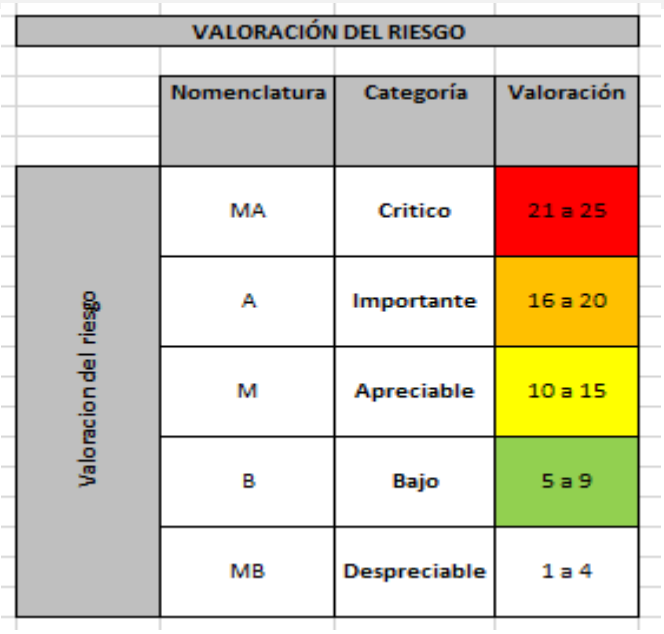
No.	DATOS DEL ACTIVO DE INFORMACION	DIMENSION				
		[A]	[T]	[C]	[I]	[D]
1	[HW] Equipo de Escritorio	MA	MB	B	B	B
2	[HW] Equipo Portatil	MA	MB	B	B	B
3	[HW] Equipo Servidor	MA	MA	MA	MA	MA
4	[HW] Sistema de Backup	M	A	A	A	A
5	[COM] Equipos de Red	MB	MA	MA	MA	MA
6	[D] Manejo de datos	A	A	A	A	A

7	[SW] Sistemas Operativos	MA	MA	MA	MA	MA
8	[SW] Lenguajes de desarrollo	MA	M	A	A	A
9	[SW] Base de datos Desarrollo	A	A	A	A	A
10	[SW] Base de datos Pruebas	A	A	A	A	A
11	[SW] Base de datos Produccion	A	A	A	A	A
12	[PERSONAL] Director TI	A	A	A	A	A
13	[PERSONAL] Analistas	MA	MA	MA	MA	MA
14	[PERSONAL] Desarroladores	MB	MB	B	B	B
15	[PERSONAL] Usuario Final	MA	MA	MA	MA	MA
16	[I] Instalaciones	M	M	MA	MA	A

Fuente: Autor

7.3. VALORACIÓN CUANTITATIVA DE ACTIVOS.

Resumen de Valoración de Riesgos de los Activos



VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Nombre	Riesgo	[A]	[T]	[C]	[I]	[D]	VALOR
[HW] Equipo de Escritorio	APRECIABLE	25	4	9	9	9	11
[HW] Equipo Portatil	APRECIABLE	25	4	9	9	9	11
[HW] Equipo Servidor	CRITICO	25	25	25	25	25	25
[HW] Sistema de Backup	IMPORTANTE	15	20	20	20	20	19
[COM] Equipos de Red	CRITICO	4	25	25	25	25	21
[D] Manejo de datos	IMPORTANTE	20	20	20	20	20	20

[SW] Sistemas Operativos	CRITICO	25	25	25	25	25	25
[SW] Lenguajes de desarrollo	IMPORTANTE	25	15	20	20	20	20
[SW] Base de datos Desarrollo	IMPORTANTE	20	20	20	20	20	20
[SW] Base de datos Pruebas	IMPORTANTE	20	20	20	20	20	20
[SW] Base de datos Producción	IMPORTANTE	20	20	20	20	20	20
[PERSONAL] Director TI	IMPORTANTE	20	20	20	20	20	20
[PERSONAL] Analistas	CRITICO	25	25	25	25	25	25
[PERSONAL] Desarrolladores	BAJO	4	4	9	9	9	7
[PERSONAL] Usuario Final	CRITICO	25	25	25	25	25	25
[I] Instalaciones	IMPORTANTE	15	15	25	25	20	20

7.4 IDENTIFICACION DE AMENAZAS.

No. De	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit
1	[HW] Equipo de Escritorio	11	[I5] Avería de origen físico o lógico
2	[HW] Equipo de Escritorio	11	[I6] Corte del suministro eléctrico
3	[HW] Equipo de Escritorio	11	[I*] Desastres industriales
4	[HW] Equipo de Escritorio	11	[A26] Ataque destructivo
5	[HW] Equipo de Escritorio	11	[A11] Acceso no autorizado
6	[HW] Equipo Portatil	11	[I5] Avería de origen físico o lógico
7	[HW] Equipo Portatil	11	[I7] Condiciones inadecuadas de temperatura o humedad
8	[HW] Equipo Portatil	11	[I6] Corte del suministro eléctrico
9	[HW] Equipo Portatil	11	[I*] Desastres industriales
10	[HW] Equipo Portatil	11	[A26] Ataque destructivo
11	[HW] Equipo Portatil	11	[A11] Acceso no autorizado
12	[HW] Equipo Servidor	25	[N1] Fuego
13	[HW] Equipo Servidor	25	[N2] Daños por agua
14	[HW] Equipo Servidor	25	[I*] Desastres industriales
15	[HW] Equipo Servidor	25	[I*] Desastres industriales
16	[HW] Equipo Servidor	25	[A11] Acceso no autorizado
17	[HW] Equipo Servidor	25	[I6] Corte del suministro eléctrico
18	[HW] Equipo Servidor	25	[E14] Escapes de información
19	[HW] Sistema de Backup	19	[E10] Errores de secuencia
20	[HW] Sistema de Backup	19	[E14] Escapes de información
21	[HW] Sistema de Backup	19	[A11] Acceso no autorizado
22	[HW] Sistema de Backup	19	[N1] Fuego
23	[HW] Sistema de Backup	19	[A25] Robo

24	[HW] Sistema de Backup	19	[E19] Fugas de información
25	[COM] Equipos de Red	21	[A11] Acceso no autorizado
26	[COM] Equipos de Red	21	[I6] Corte del suministro eléctrico
27	[COM] Equipos de Red	21	[I*] Desastres industriales
28	[COM] Equipos de Red	21	[A26] Ataque destructivo
29	[COM] Equipos de Red	21	[A11] Acceso no autorizado
30	[D] Manejo de datos	20	[E1] Errores de los usuarios
31	[D] Manejo de datos	20	[E2] Errores del administrador
32	[D] Manejo de datos	20	[A5] Suplantación de la identidad del usuario
33	[D] Manejo de datos	20	[A8] Difusión de software dañino
34	[D] Manejo de datos	20	[A15] Modificación deliberada de la información
35	[D] Manejo de datos	20	[A26] Ataque destructivo
36	[D] Manejo de datos	20	[A11] Acceso no autorizado
37	[D] Manejo de datos	20	[E19] Fugas de información
38	[SW] Sistemas Operativos	25	[A11] Acceso no autorizado
39	[SW] Sistemas Operativos	25	[A26] Ataque destructivo
40	[SW] Sistemas Operativos	25	[E2] Errores del administrador
41	[SW] Lenguajes de desarrollo	20	[A11] Acceso no autorizado
42	[SW] Lenguajes de desarrollo	20	[A26] Ataque destructivo
43	[SW] Lenguajes de desarrollo	20	[E2] Errores del administrador
44	[SW] Base de datos Desarrollo	20	[A11] Acceso no autorizado
45	[SW] Base de datos Desarrollo	20	[A26] Ataque destructivo
46	[SW] Base de datos Desarrollo	20	[E2] Errores del administrador
47	[SW] Base de datos Desarrollo	20	[A15] Modificación deliberada de la información
48	[SW] Base de datos Desarrollo	20	[A24] Denegación de servicio
49	[SW] Base de datos Pruebas	20	[A11] Acceso no autorizado
50	[SW] Base de datos Pruebas	20	[A26] Ataque destructivo
51	[SW] Base de datos Pruebas	20	[E2] Errores del administrador
52	[SW] Base de datos Pruebas	20	[A15] Modificación deliberada de la información
53	[SW] Base de datos Pruebas	20	[A24] Denegación de servicio
54	[SW] Base de datos Produccion	20	[A11] Acceso no autorizado
55	[SW] Base de datos Produccion	20	[A26] Ataque destructivo
56	[SW] Base de datos Produccion	20	[E2] Errores del administrador
57	[SW] Base de datos Produccion	20	[A15] Modificación deliberada de la información
58	[SW] Base de datos Produccion	20	[A24] Denegación de servicio
59	[PERSONAL] Director TI	20	[A22] Manipulación de programas
60	[PERSONAL] Director TI	20	[A19] Divulgación de información
61	[PERSONAL] Director TI	20	[A18] Destrucción de información
62	[PERSONAL] Director TI	20	[A14] Interceptación de información (escucha)
63	[PERSONAL] Analistas	25	[A23] Manipulación de los equipos
64	[PERSONAL] Analistas	25	[A11] Acceso no autorizado
65	[PERSONAL] Analistas	25	[A6] Abuso de privilegios de acceso
66	[PERSONAL] Analistas	25	[A5] Suplantación de la identidad del usuario
67	[PERSONAL] Analistas	25	[A4] Manipulación de la configuración
68	[PERSONAL] Desarroladores	7	[A23] Manipulación de los equipos
69	[PERSONAL] Desarroladores	7	[A11] Acceso no autorizado

70	[PERSONAL] Desarroladores	7	[A6] Abuso de privilegios de acceso
71	[PERSONAL] Desarroladores	7	[A5] Suplantación de la identidad del usuario
72	[PERSONAL] Desarroladores	7	[A4] Manipulación de la configuración
73	[PERSONAL] Usuario Final	25	[A24] Denegación de servicio
74	[PERSONAL] Usuario Final	25	[A11] Acceso no autorizado
75	[I] Instalaciones	20	[A26] Ataque destructivo
76	[I] Instalaciones	20	[A5] Suplantación de la identidad del usuario
77	[I] Instalaciones	20	[N1] Fuego
78	[I] Instalaciones	20	[N2] Daños por agua
79	[I] Instalaciones	20	[N*] Desastres naturales
80	[I] Instalaciones	20	[A26] Ataque destructivo

7.5. ESTADO Y APLICABILIDAD DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ANEXO A ISO 27002:2013

Sección	Controles de Seguridad de la Información	Estado	Recurso
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información	Inicial	
A5.1.2	Revisión de las políticas para la seguridad de la información	Inicial	
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información	Definido	
A6.1.2	Segregación de tareas	Inexistente	
A6.1.3	Contacto con las autoridades	Inexistente	
A6.1.4	Contacto con grupos de interés especial	Inexistente	
A6.1.5	Seguridad de la información en la gestión de proyectos	Inicial	
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles	Inexistente	
A6.2.2	Teletrabajo	Inexistente	
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	Definido	
A7.1.2	Términos y condiciones del empleo	Inexistente	
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	Inexistente	
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inexistente	
A7.2.3	Proceso disciplinario	Inexistente	
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	Inexistente	
A8	**Gestión de activos**		

A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	Definido	
A8.1.2	Propiedad de los activos	Definido	
A8.1.3	Uso aceptable de los activos	Inicial	
A8.1.4	Devolución de activos	Inicial	
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	Definido	
A8.2.2	Etiquetado de la información	Definido	
A8.2.3	Manipulado de la información	Definido	
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	Definido	
A8.3.2	Eliminación de soportes	Inexistente	
A8.3.3	Soportes físicos en tránsito	Inexistente	
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Inicial	
A9.1.2	Acceso a las redes y a los servicios de red	Inicial	
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	Inicial	
A9.2.2	Provisión de acceso de usuario	Inicial	
A9.2.3	Gestión de privilegios de acceso	Inicial	
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inicial	
A9.2.5	Revisión de los derechos de acceso de usuario	Inicial	
A9.2.6	Retirada o reasignación de los derechos de acceso	Inicial	
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	Definido	
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	Inicial	
A9.4.2	Procedimientos seguros de inicio de sesión	Definido	
A9.4.3	Sistema de gestión de contraseñas	Definido	
A9.4.4	Uso de utilidades con privilegios del sistema	Inicial	
A9.4.5	Control de acceso al código fuente de los programas	Inicial	
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos	Inexistente	
A10.1.2	Gestión de claves	Inexistente	
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	Inexistente	
A11.1.2	Controles físicos de entrada	Inexistente	
A11.1.3	Seguridad de oficinas, despachos y recursos	Inexistente	

A11.1.4	Protección contra las amenazas externas y ambientales	Inexistente	
A11.1.5	El trabajo en áreas seguras	Inexistente	
A11.1.6	Áreas de carga y descarga	Inexistente	
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	Inexistente	
A11.2.2	Instalaciones de suministro	Inicial	
A11.2.3	Seguridad del cableado	Inexistente	
A11.2.4	Mantenimiento de los equipos	Inexistente	
A11.2.5	Retirada de materiales propiedad de la empresa	Inexistente	
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Inexistente	
A11.2.7	Reutilización o eliminación segura de equipos	Inexistente	
A11.2.8	Equipo de usuario desatendido	Inexistente	
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Inexistente	
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales	Inexistente	
A12.1.2	Gestión de cambios	Inexistente	
A12.1.3	Gestión de capacidades	Inexistente	
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Inexistente	
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso	Inicial	
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	Inexistente	
A12.4	**Registros y supervisión**		
A12.4.1	Registro de eventos	Inexistente	
A12.4.2	Protección de la información del registro	Inexistente	
A12.4.3	Registros de administración y operación	Inexistente	
A12.4.4	Sincronización del reloj	Inexistente	
A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación	Inexistente	
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Inexistente	
A12.6.2	Restricción en la instalación de software	Inexistente	
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	Inexistente	
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	Inicial	
A13.1.2	Seguridad de los servicios de red	Inicial	
A13.1.3	Segregación en redes	Inicial	
A13.2	**Intercambio de información**		

A13.2.1	Políticas y procedimientos de intercambio de información	Inexistente	
A13.2.2	Acuerdos de intercambio de información	Inicial	
A13.2.3	Mensajería electrónica	Inicial	
A13.2.4	Acuerdos de confidencialidad o no revelación	Inicial	
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Inicial	
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Inicial	
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Inicial	
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	Inicial	
A14.2.2	Procedimiento de control de cambios en sistemas	Inicial	
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Inicial	
A14.2.4	Restricciones a los cambios en los paquetes de software	Inicial	
A14.2.5	Principios de ingeniería de sistemas seguros	Inexistente	
A14.2.6	Entorno de desarrollo seguro	Inexistente	
A14.2.7	Externalización del desarrollo de software	Inexistente	
A14.2.8	Pruebas funcionales de seguridad de sistemas	Inexistente	
A14.2.9	Pruebas de aceptación de sistemas	Definido	
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	Inicial	
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Inexistente	
A15.1.2	Requisitos de seguridad en contratos con terceros	Inexistente	
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Inexistente	
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Inexistente	
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Inexistente	
A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos	Inicial	
A16.1.2	Notificación de los eventos de seguridad de la información	Inicial	
A16.1.3	Notificación de puntos débiles de la seguridad	Inicial	
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Inicial	
A16.1.5	Respuesta a incidentes de seguridad de la información	Inicial	
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inicial	
A16.1.7	Recopilación de evidencias	Inicial	

A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Inicial	
A17.1.2	Implementar la continuidad de la seguridad de la información	Inicial	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Inicial	
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Inexistente	
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Inicial	
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Inexistente	
A18.1.3	Protección de los registros de la organización	Inicial	
A18.1.4	Protección y privacidad de la información de carácter personal	Inicial	
A18.1.5	Regulación de los controles criptográficos	Inexistente	
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	Inicial	
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Inicial	
A18.2.3	Comprobación del cumplimiento técnico	Inicial	

Tabla 6 Controles
Fuente: Autor

8. GUIA DE POLITICAS Y BUENAS PRACTICAS

8.1 DEFINICIONES.

A continuación, se realiza la definición de los conceptos relacionados con el Gobierno de datos.

Activos de Información: Cualquier información (conjunto de datos) o elemento relacionado con la gestión de estos (sistemas de información, medios de salvaguardo, instalaciones y/o usuarios) y posean valor para la organización.

Propietario de la información: Persona encargada de la gestión de la integridad, disponibilidad y confiabilidad de la información de la empresa.

Custodio de Información: Persona encargada de la protección y salvaguarda de la información, debe crear, implementar y auditar los controles necesarios para mantener protegida la información.

Arquitectura de datos: Es lo relacionado a la estructura de los almacenes de datos, semántica y calidad del dato en todo su ciclo de vida.

Calidad del dato: Es el proceso asociado con procesos al ajuste, depuración de datos masivos, definición, medición y mejora continua de los indicadores de calidad del dato.

Ciclo de vida de la información: Son los estados de la gestión del dato los cuales son: creación, procesamiento, almacenamiento, trasmisión y disposición final.

Dato maestro: Es aquel dato preciso y específico.

Gestión del dato: Es la actividad que debe asegurar, mantener y proveer la información, unificando datos maestros y estandarizando registros en los sistemas fuente.

Gobierno del dato: Es una disciplina clave para controlar el uso de los datos maestros. El gobierno aborda los ámbitos de arquitectura, calidad, custodia, aprovisionamiento, seguridad y privacidad y gestión de la demanda del dato.

Metadatos: Definiciones de datos empresariales que ayudan a establecer el contexto de los datos y así contribuir directamente a mejorar la calidad de la información.

8.2 POLÍTICAS GENERALES.

Se definen los siguientes principios y políticas del gobierno de datos:

8.3.1 ESTRATEGIA DE DATOS.

Se debe garantizar las necesidades estratégicas de la información, asegurando que se tiene en cuenta lo requerido para alcanzar los objetivos estratégicos de la empresa en cuanto a la seguridad, confiabilidad y disponibilidad de la información.

8.3.2 RESPONSABILIDAD Y PROPIEDAD DE LOS DATOS.

Se debe definir los propietarios por cada uno de los activos de información identificados en la empresa para asegurar la integridad, confidencialidad, disponibilidad, privacidad y la calidad en el contenido de los datos.

8.3.3 ROLES Y ORGANIZACIONES DE PROFESIONALES DE DATOS

Definir formalmente los roles de carácter técnico, necesarios para gestión de los datos con el fin de facilitar la gobernabilidad del modelo de gestión del dato.

8.3.4 GESTIÓN DE PROYECTOS DE DATOS.

Se debe establecer y mantener un portafolio de proyectos e iniciativas relacionados con la gestión de datos, que permitirá definir un curso de acción para su mejoramiento a través de una hoja de ruta.

8.3.5 CATÁLOGO DE SERVICIOS DE DATOS.

Crear y mantener portafolio que formalice las actividades asociadas a la gestión y gobierno de datos indicando los servicios proporcionados, las áreas responsables y los acuerdos de nivel de servicios.

8.3.6 ARQUITECTURA Y GESTIÓN DE METADATOS.

Definir la arquitectura de datos, identificando y caracterizando los activos de información a través de procesos formales, para facilitar la disponibilidad, acceso, uso e intercambio por medio de un modelo de datos empresarial el cual estará alineado con la estrategia de negocio.

8.3.7 DATOS MAESTROS, REFERENCIALES Y GESTIÓN DE DOCUMENTOS Y CONTENIDOS DE DATOS.

Se debe definir los procesos, procedimientos y controles necesarios para la adecuada gestión de los datos maestros, datos no estructurados (documentos, audios, videos, imágenes) tanto físico como digitales, especialmente los relacionados con el asociado, cliente, usuario, empleado y demás entidades de datos definidas, que permita el control sobre el almacenamiento, protección y acceso de los datos con el fin de proporcionar una fuente autorizada de datos conciliados de alta calidad, reducir su costo y complejidad mediante la reutilización, el apalancamiento de estándares, apoyando los esfuerzos de integración de la información, de inteligencia empresarial para garantizar la seguridad y privacidad de la información.

8.3.8 RESPONSABLES DEL GOBIERNO DE DATOS.

Se define la siguiente estructura responsable de la gestión, implementación, control y cumplimiento del gobierno de datos, con las funciones y responsabilidades que más adelante se indican:

Comité Corporativo de Gobierno de Datos
CIO (Chief Information Officer)
Comité Corporativo de Gestión de Datos

8.3.8.1 COMITÉ CORPORATIVO DE GOBIERNO DE DATOS.

Será el responsable de:

a) Proponer los ajustes de las políticas del gobierno de los datos.
b) hacer seguimiento a las métricas de gobierno, gestión de datos y aprobar cambios al modelo de datos empresarial.
c) Revisar los informes de avance y las diferentes.
d) Actividades de implementación realizadas.
e) Validar los procesos propuestos, herramientas, metodologías e indicadores, presentar a la Alta Gerencia conclusiones y recomendaciones de los hechos más representativos en la ejecución de las actividades de la implementación del Programa.

8.3.8.2 CIO (Chief Information Officer).

Es el responsable de la gestión de las tecnologías de información y los sistemas que soportan los objetivos de la organización.

8.3.8.3 COMITÉ CORPORATIVO DE GESTIÓN DE DATOS.

Será el responsable de garantizar la implementación de actividades de gestión de datos. El comité se reunirá ordinariamente de forma mensual o con la frecuencia que se considere necesaria.

8.3.9 MONITOREO, SEGUIMIENTO Y CONTROL.

Se debe realizar seguimiento y mejoramiento a las políticas y buenas prácticas planteadas.

9. RESULTADOS OBTENIDOS.

La puesta en marcha de las políticas en el marco del Gobierno de datos no es una tarea sencilla, requiere la capacitación ay aceptación de todos los involucrados desde la alta gerencia hasta el analista de datos que desarrolla los procesos de Inteligencia de Negocio para la empresa; pero el premio es que si todo el proceso de implementación se lleva a cabo, la empresa mejora el nivel de seguridad de sus datos, logrando actividades de desarrollo de Inteligencia de Negocios más rápidos y ceñidos a los pilares fundamentales de la seguridad informática que son:; Integridad, Disponibilidad y Confidencialidad.

En este capítulo se definen los factores de éxito en la implementación de las políticas en el gobierno de datos en desarrollos BI, las siguientes son las recomendaciones:

1. Definir los objetivos del desarrollo BI dentro de la empresa, estos deben estar alineados a la misión de la empresa, deben se la razón de existir.

2. Realizar el inventario de los activos informáticos de la empresa, se debe conocer exactamente con que se cuenta y donde están ubicados, definiendo detalladamente lo servidores de datos, de aplicación y computadores personales o herramientas para acceder a los reportes fínanles producto del desarrollo del BI empresarial

10. CONCLUSIONES.

- El diseño de las políticas y buenas prácticas en el desarrollo de soluciones de inteligencia de negocios BI permite a los analistas BI mecanismos de protección de los datos y control de los riesgos y vulnerabilidades identificados en el desarrollo de la metodología MAGERIT.

- La aplicación de la metodología MAGERIT permite identificar los riesgos y vulnerabilidades a los que se encuentran expuesta los datos en el desarrollo de soluciones BI haciendo posible determinar las políticas y estrategias de desarrollo para la protección de la información.

- Las políticas establecidas se crean con el propósito de motivar a los analistas de desarrollo de BI a adoptarlas y de esta forma lograr seguridad en el desarrollo y manipulación de los datos, teniendo en cuenta los tres principios de la seguridad: integridad, disponibilidad y confidencialidad.

- Los datos de una organización siempre tendrán ciberdelincuentes al acecho, la implementación de la metodología MAGERIT y la adopción de las políticas de seguridad hacen que se tenga una buena seguridad en las aplicaciones BI.

11. RECOMENDACIONES.

- Concienciar a las entidades públicas y privadas frente a la necesidad de implementar políticas y buenas prácticas de gobierno de datos en el desarrollo de sus proyectos de Inteligencia de Negocios, frente a la seguridad de la información y los datos que allí se manejan.

- A las entidades públicas y privadas, la puesta en marcha de políticas y buenas prácticas de gobierno de datos tanto en el desarrollo de proyectos de inteligencia de negocios (BI), como en la seguridad de la información y los datos que allí se implementen, siendo vinculante dentro del diseño de dichas políticas el estudio de las mejores prácticas de seguridad y de gobierno TI propuestas por los estándares ISO internacionales.

- La creación de un documento unificado para las empresas, donde se articulen las políticas y buenas prácticas de gobierno de datos en el desarrollo de proyectos de inteligencia de negocios (BI), mediante la metodología MAGERIT con la de Seguridad de la Información y los datos, Ciberseguridad y el de Inteligencia Artificial (IA).

BIBLIOGRAFIA

ÁLVAREZ, Carlos. Pronunciamiento sobre ley de Habeas Data [en línea]. EL TIEMPO, mayo de 2007 [Consultado 29 de marzo de 2019]. Disponible en Internet: http://blogs.eltiempo.com/el-lado-oscuro-de-internet/2007/05/31/pronunciamiento-sobre-ley-de-habeas-data/

ARENAS ROSERO, Javier. La influencia de los softwares de Business Intelligence en la optimización de los tiempos de respuesta operacionales. Facultad De Ciencias Económicas Y Administrativas Carrera De Administración De Empresas Bogotá D.C, 2018. 57 p.

BECKER, J. e. 2009. Developing a Framework for IT Governance in the postmerger integration phase. 17th European Conference on Information Systems. Verona: Scholar One.

BELLO, D., DANT, S., & LOHTIA, R. (1997). Hybrid governance: the role of transaction costs, production costs and strategic considerations. Journal of Business and Industrial Marketing, 12, 118-133.

BERSON, Alex. Master Data Management And Data Governance. Second Edition, United State of America, Mc Graw - Hill, 2011. 467 p. ISBN: 0071744584.

Beyond Volume, Variety and Velocity is the Issue of Big Data Veracity. [en línea] [Consultado 17 de marzo de 2019] Disponible en: https://insidebigdata.com/2013/09/12/beyond-volume-variety-velocity-issue-big-data-veracity/

CALLE D' ALEMAN, Sol Beatriz. Protección de datos personales en la banca electrónica a la luz del actual proyecto de habeas data en Colombia [en línea]. Universidad Externado de Colombia, sin fecha [Consultado 29 de marzo de 2017]. Disponible en Internet: https://www.uexternado.edu.co/wp-content/uploads/2017/01/Proteccion-de-datospersonales-a-la-luz-del-Proyecto-de-Ley-de-habeas-data-en-Colombia.doc.

CAMARGO BEDOYA, Carlos Andrés. Solución informática de gestión de datos personales del ciudadano colombiano. Para optar al título de Magister en Ingeniería de Sistemas. Pontificia Universidad Javeriana. Facultad De Ingeniería. Carrera De Ingeniería De Sistemas, Bogotá, 2014. 94 p.

CAVIEDES VARGAS, Andrés Felipe. MURILLO REALES, Javier Alejandro. Gobierno de ti en pymes: estado actual del gobierno de ti en empresas privadas de seguridad en Bogotá. Trabajo de investigación para optar al Título de Ingeniero de Sistemas. Universidad Católica De Colombia. Facultad de ingeniería. Programa de ingeniería de sistemas. BOGOTÁ, 2014. 99 p

CHAVES ROSERO, Mario Andrés. Resguardar la información del sistema de gestión documental Document en la Empresa Contactar - Pasto, Trabajo de grado para optar al título de especialista en Seguridad informática. Universidad Nacional Abierta Y A Distancia UNAD. Escuela de ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad informática, Bogotá, 2017. 111 p.

CORDOBA ARAUJO, Leyda Liliana, DELGADO TRUJILLO. Wilson Camilo Diseño de las políticas de control de riesgos de la seguridad de la información para la sede central de la gobernación del Putumayo (Mocoa). Trabajo de grado para optar al título de especialista en Seguridad informática. Universidad Nacional Abierta Y A Distancia UNAD. Escuela de ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad informática, Bogotá, 2016. 179 p.

3D Data Management: Controlling Data Volume, Velocity and Variety", [en línea] [Consultado 17 de marzo de 2019] Disponible en: http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3DData-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

Dezyre, Inteligencia de negocios. Caso Walmart [consultado el 15 de mayo de 2019] Disponible en https://www.dezyre.com/article/how-big-data-analysis-helped-increase-walmarts-sales-turnover/109

El volumen de datos almacenados en Internet será 44 veces mayor en 2020, [en línea] [Consultado 17 de marzo de 2019] Disponible en: http://www.elmundo.es/elmundo/2013/07/30/navegante/1375199227.html

FERNANDEZ BERNAL, Camilo. Guía de buenas prácticas de seguridad en el desarrollo de software con base en estándares reconocidos en empresas de desarrollo de software. Trabajo de grado para optar al título de especialista en Seguridad informática. Universidad Nacional Abierta Y A Distancia UNAD. Escuela de ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad informática, Risaralda, 2018. 118 p.

Gobierno de Datos. [en línea]. [Consultado 09 de febrero de 2019]. Disponible en: https://m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2019/CIGRAS-2019.09.09-03-Gobierno%20de%20datos-Gustavo%20Mesa-Hector%20Cotelo.pdf

HEFLOS. Que es Gobierno de Datos [en línea] 10 de noviembre de 2017 [Consultado 09 de febrero de 2019] Disponible en: https://www.heflo.com/es/blog/gobernanza/gobierno-dados/

HENDERSON, Deborah. Data Management Body of Knowledge. Second Edition. United State of America: DAMA-DMBOK, 2017. 615 p. ISBN: 9781634622349

IBM. Seis pasos para el Gobierno de Datos [en línea] marzo de 2012. [Consultado 09 de febrero de 2019] Disponible en: https://www.ibm.com/developerworks/ssa/data/library/techarticle/gobierno-datos/index.html

INSTITUTO POLITÉCNICO NACIONAL. Aplicación de inteligencia de negocios haciendo uso del data Warehouse 2.0 en la empresa constructora Beaver para mejorar el proceso de control de información de los centros de costos, Bach. TUÑOQUE JULCAS, MARTHA LUZ, Bach. VILCHEZ ZAPATA, OSWALDO [en línea] 29 de octubre de 2016. [Consultado 09 de febrero de 2019] Disponible en: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/327/VALDIVIEZO_MANUEL_AN%C3%81LISIS_Y_DISE%C3%91O_DE_UNA_HERRAMIENTA_DE_DESARROLLO_DE_SOLUCIONES_PARA_INTELIGENCIA_DE_NEGOCIOS_AN%C3%81LISIS_DIMENSIONAL.pdf?sequence=1

INSTITUTO POLITÉCNICO NACIONAL. Una Gestión De Datos Para Mejorar Y Dar Soporte A La Toma De Decisiones En Los Negocios, CESAR ALEJANDRO CASTILLO ALVARADO [en línea] 29 de octubre de 2016. [Consultado 09 de febrero de 2019] Disponible en: http://148.204.210.201/tesis/1442331060889TTv.pdf

ISACA. Gobierno de Datos [en línea] 16 de abril de 2014 [Consultado 09 de febrero de 2019] Disponible en: https://m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2019/CIGRAS-2019.09.09-03-Gobierno%20de%20datos-Gustavo%20Mesa-Hector%20Cotelo.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la información (SGSI). Bogotá: ICONTEC, 2004, 67 p. (NTC-BS 7799-2)

ISO 17799. SEGURIDAD DIGITAL [en línea] [Consultado 10 de marzo de 2019]. Disponible en: https://cincodias.elpais.com/cincodias/2009/02/27/empresas/1235745603_850215.html

ISACA Manuel Ballester PhD,
Gobierno de las TIC ISO/IEC 38500. The ISACA Journal [en línea] [Consultado 29 de marzo de 2019]. Disponible en: http://www.isaca.org/Journal/Past-Issues/2010/Volume1/Documents/jpdf1001onlinegobierno.pdf

La gestión del Big Data en la inteligencia de negocio. Caso Walmart [en línea]. [Consultado 09 de febrero de 2019]. Disponible en: http://blogs.icemd.com/blog-la-gestion-del-big-data-en-la-inteligencia-de-negocio-/el-caso-walmart/

LADLEY, John. Data Governance: How to Design, Deploy and Sustain and Effective

Data Governance Program. First Edition, United State of America: The Morgan Kaufmann Series on Business Intelligence, 2012. 258 p. ISBN 10: 0124158293

Ley 1273 5 de enero de 2009. Por Medio De La Cual Se Modifica El Código Penal, Se Crea Un Nuevo Bien Jurídico Tutelado - Denominado "De La Protección De La Información Y De Los Datos"· Y Se Preservan Integralmente Los Sistemas Que Utilicen Las Tecnologías De La Información Y Las Comunicaciones, Entre Otras Disposiciones. [en línea] [Consultado 27 de marzo de 2019] Disponible en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

LOSADA RIVERA, Javier Alejandro. OLIVERA ARBOLEDA, Marco Antoni. Propuesta para el cumplimiento de los controles técnicos de la circular 14 basado en el modelo planteado por la Norma ISO 27001, bajo plataforma Oracle. Para optar al título de ingeniero de sistemas. Pontificia Universidad Javeriana. Facultad De Ingeniería Carrera De Ingeniería De Sistemas. Bogotá, 2010 95 p.

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. (2012). Sistema de Información Unificado del Sector de Telecomunicaciones - SIUST. [en línea] [Consultado 15 de Marzo de 2019] Disponible en: http://www.siust.gov.co/siust/

MAHECHA MERA, Heiner. Implementación de una herramienta “Dashboard” para el control y gestión de procesos automatizados en Colpensiones. Trabajo de grado para optar al título de especialista en Seguridad informática. Universidad Nacional Abierta Y A Distancia UNAD. Escuela de ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad informática, Bogotá, 2017. 125 p.

ORTIZ PULIDO, Andrea Patricia. CORREDOR MERCHÁN, Jonnathan Silvestre. Sistema de anonimización de datos estructurados. Pontificia Universidad Javeriana. Facultad De Ingeniería. Maestría En Ingeniería De Sistemas Y Computación. Bogotá, 2017. 885 p.

P. Ashley, S. Hada, G. Karjoth, C. Powers, y M. Schunter, «The Enterprise Privacy Authorization Language (EPAL). [en línea]. [Consultado 29 de marzo de 2019] Disponible en: https://www.w3.org/2003/p3p-ws/pp/ibm3.html

Pandorafms, “NOSQL vs SQL. Diferencias y cuando elegir cada una”, [en línea] [Consultado 17 de marzo de 2019] Disponible en: http://blog.pandorafms.org/es/nosql-vs-sql-diferenciasy-cuando-elegir-cada-una/

PRADA HERNÁNDEZ, Nathalia Milena. Diseño De Un Sistema De Gestión De Seguridad De La Información, Alineado Con La Norma ISO/IEC 27002, Para El Área De Tecnología De Una Empresa Del Sector Financiero. Para optar al título de ingeniero de sistemas. Pontificia Universidad Javeriana. Facultad De Ingeniería. Carrera De Ingeniería De Sistemas, Bogotá, 2010. 93 p.

Procesos ETL: Extracción, Transformación, Carga. [en línea] [Consultado 15 de marzo de 2019]. Disponible en: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/288859/procesos-etl-extracci-n-transformaci-n-carga

Principios de diseño para procesos de ETL. [en línea] [Consultado 15 de marzo de 2019]. Disponible en: file:///D:/Trabajos%20Universidad/Seguridad%20Informatica/Juan%20David%20Cardona/Semestre%202/PROYECTO%20DE%20SEGURIDAD%20INFORMATICA%20I/insumos/45629_Principios_de_dise%C3%B1o_para_procesos_de_ETL.pdf

Proyecto de ley 241 de 2011 senado [en línea] [Consultado 27 de marzo de 2019] Disponible https://vlex.com.co/vid/proyecto-ley-senado-451474518

RINCON DANIEL, Nicolle Smith. VILLARREAL MONTAÑEZ, Alexander. El registro de bases de datos como garantía de la protección de datos personales. Monografía Jurídica para optar al título de Abogados. Pontificia Universidad Javeriana. Facultad De Ciencias Jurídicas. Departamento De Derecho Privado. Bogotá, 2017. 96 p.
SAS Institute, «SAS® Help Center: Data Mining and SEMMA». [en línea]. [Consultado 13 de marzo de 2019] Disponible en: http://documentation.sas.com/?docsetId=emcs&docsetTarget=n0pejm83csbja4n1xueveo2uoujy.htm&docsetVersion=12.3&locale=en.

SAS. Impida que el "gobierno de datos" se convierta en un dolor de cabeza en su organización [en línea] 16 de abril de 2014 [Consultado 09 de febrero de 2019] Disponible en: https://blogs.sas.com/content/sasla/2014/04/16/gobierno-de-datos/

SOARES, Sunil. The IBM Data Governance Unified Process. First Edition, United State of America: MC Press On Line, LLC, 2010. 168 p. ISBN: 978-158347-360-3

SOARES, Sunil. The Chief Data Officer Handbook for Data Governance. United State of America, 2014. P. ISBN 978-1-5834-417-4

SOARES, Sunil. Big Data Governance: An Emerging Imperative, First Edition, United State of America, MC Press On Line, LLC, 2012. p. ISBN: 978-1-588347-377-1.

TEMPLAR, Morgan. Get Governed: Building World Class Data Governance Programs. First Edition, United State of America: Ivory Lady Publishihing, 2017. 276 p. ISBN 10: 0692952175X

UCI Machine Learning Repository. [en línea]. [Consultado 13 de marzo de 2019] Disponible en: https://archive.ics.uci.edu/ml/index.php.

UNIVERSIDAD INTERNACIONAL DE VALENCIA. Conceptos sobre seguridad lógica informática. [en línea] Marzo, 2018. [Consultado 09 de febrero de 2019]. Disponible en: https://www.universidadviu.com/conceptos-seguridad-logica-informatica/

UNIVERSIDAD CESAR VALLEJO. Inteligencia de negocios en la gestión del conocimiento del área de informática del servicio de traumatología del Hospital Arzobispo Loayza, Lima - 2017, Marcelo Leonardo Espíritu Isidro, [en línea] 15 de octubre de 2017. [Consultado 09 de febrero de 2019] Disponible en: http://repositorio.ucv.edu.pe/bitstream/handle/UCV/15683/Esp%C3%ADritu_IML.pdf?sequence=1&isAllowed=y

UNIVERSIDAD IGNACIO DE LOYOLA. Implementación De Inteligencia De Negocios Para El Área Comercial De La Empresa Azaleia - Basado En Metodología Ágil Scrum, SALAZAR TATAJE, Jubitza Lisbeth, [en línea] 15 de octubre de 2017. [Consultado 09 de febrero de 2019] Disponible en: http://repositorio.usil.edu.pe/bitstream/USIL/2896/1/2017_Salazar_Implementacion-de-inteligencia-de-negocios.pdf

URIBE OTÁLORA, Carlos. Estudio de seguridad informática para las bases de datos del campus virtual de la UNAD, Trabajo de grado para optar al título de especialista en Seguridad informática. Universidad Nacional Abierta Y A Distancia UNAD. Escuela de ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad informática, Bogotá, 2016. 85 p.

Villarroel, Rodolfo & Gómez, Yessica & Krause, Constanza. (2012). Incorporación de Seguridad en el Modelado Conceptual de Procesos Extracción-Transformación-Carga. Información tecnológica. [en línea]. [Consultado 17 de marzo de 2019] Disponible en: https://www.researchgate.net/publication/262472831_Incorporacion_de_Seguridad_en_el_Modelado_Conceptual_de_Procesos_Extraccion-Transformacion-Carga