ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE SISTEMAS

UNIDAD DE TITULACIÓN

DISEÑO DE UN MARCO DE TRABAJO PARA EL ANÁLISIS DE IMPACTO DEL PROYECTO DE LEY DE PROTECCIÓN DE DATOS EN EL ECUADOR EN EMPRESAS PRIVADAS.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN SISTEMAS DE INFORMACIÓN MENCIÓN INTELIGENCIA DE NEGOCIOS Y ANALITICA DE DATOS MASIVOS

MARCO VINICIO BURBANO SÁNCHEZ
marco.burbano1@epn.edu.ec

Director: Marco Antonio Segura Morales, PhD
marco.segura@epn.edu.ec

Codirector: Edison Fernando Loza Aguirre, PhD
edison.loza@epn.edu.ec

2021

APROBACIÓN DEL DIRECTOR

Como director del trabajo de titulación “Marco De Trabajo Para El Análisis De Impacto Del Proyecto De Ley De Protección De Datos En El Ecuador” desarrollado por Marco Vinicio Burbano Sánchez estudiante de la Maestría de Sistemas de Información mención Inteligencia de Negocios y Análisis de Datos Masivos, habiendo supervisado la realización de este trabajo y realizado las correcciones correspondientes, doy por aprobada la redacción final del documento escrito para que prosiga con los trámites correspondientes a la sustentación de la Defensa oral.

Marco Antonio Segura, PhD

DIRECTOR

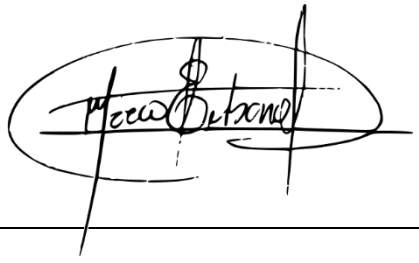
Edison Loza Aguirre, PhD

DIRECTOR

DECLARACIÓN DE AUTORÍA

Yo, Marco Vinicio Burbano Sánchez declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.



Marco Vinicio Burbano Sánchez

DEDICATORIA

A mi Esposa: Grace de Lourdes Guerrero Agila

Por haber aportado con su cariño permanente, su solidaridad y ayuda constante, durante el tiempo de mi formación.

A mis Padres:

Ejemplo de honradez y trabajo constante, para sus hijos, quienes siempre se ha esforzado por el engrandecimiento de su hogar.

AGRADECIMIENTO

A la Escuela Politécnica Nacional. Con profunda y emotiva gratitud para mis profesores, quienes me proporcionaron su tiempo, dedicación y sus sabios conocimientos.

Mi agradecimiento especial al Dr. Marco Segura, y al Dr. Edison Loza, por su acertada dirección en el desarrollo de este trabajo, cuyas valiosas sugerencias y guía constante fueron de vital importancia para la feliz culminación de la misma.

A las empresas que me permitieron desarrollar el proyecto dentro de sus instalaciones y en especial a Carlos Xavier Román y Andrés Oquendo, por su confianza al permitirme realizar mi trabajo con su equipo de trabajo y ver culminado mi proyecto profesional.

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

En el presente trabajo se realiza el análisis de la Ley Orgánica de protección de datos personales en el Ecuador y su impacto en las empresas, generando un marco de trabajo que considere la transformación empresarial que se debe desarrollar para la adopción y aplicación de la ley. Se consideran los cambios tanto interno como externo que las empresas deben realizar para cumplir con los requisitos planteados. En este sentido se aplica Arquitectura Empresarial como un marco de trabajo para el entendimiento de una organización, a través de sus entidades, relaciones, entorno y los principios de gobierno y evolución de esta. Mediante este marco de trabajo se aplica la gestión del cambio y se genera la guía para la implementación de la normativa de protección de datos.

Palabras clave: Protección de Datos, Arquitectura Empresarial, Transformación empresarial, Framework, Privacidad de Datos, Cumplimiento.

ABSTRACT

This work analyses how the law for data protection in Ecuador impacts on private businesses. We propose a Framework that considers the enterprise transformation to be developed for the adoption and application of this law. In our proposal, we considered internal and external changes that companies should implement to comply with the stated requirements. In this context, Enterprise Architecture is applied to understand organizations, through its entities, relationships, environment, governance principles and evolution. A gap is stablished for each company and later a roadmap is proposed for the implementation of all changes related with the compliance of the data protection law.

Keywords: Data Protection, Enterprise Architecture, Business Transformation, Business Architecture, Framework.

1. INTRODUCCIÓN

Actualmente, temas como la hiperconectividad, el Internet, las redes sociales y la información; han pasado de ser temas lejanos y manejados por un selecto grupo de personas, a convertirse en temas comunes y altamente utilizados para facilitar las actividades de individuos y organizaciones [1]. El uso creciente de la tecnología, sumado a su inherente evolución, han representado grandes beneficios para la sociedad; entre los cuales podemos citar mejoras a la salud, al transporte, a la educación y al manejo de energía; a tal punto que actualmente sin tecnología, no podríamos administrar por ejemplo el tráfico de ciudades o los costos de servicios de salud sin estos recursos. Por tanto, hoy en día, la tecnología es un habilitante necesario para garantizar una buena calidad de vida a los seres humanos [2].

Sin embargo, no debemos olvidar que gracias a que los datos son ahora un activo digital de gran valor económico y estratégico para varias empresas, esto ha generado también un creciente uso de los mismos de maneras poco éticas e incluso riesgosas para las personas a quien les corresponde e identifica dichos datos [3]. Así, en el año 2019 se presentaron varias denuncias de la filtración de datos de más de 20 millones de ecuatorianos según un informe de vpnMentor [4]. Este informe señalaba que la filtración incluía registros con información sociodemográfica, financiera, económica, personal e incluso de parentescos entre cada ciudadano del Ecuador. Toda esta filtración se produjo como resultado de la casi completa libertad que se tiene para el uso de la información, sumado con el desconocimiento que tienen los usuarios al momento de compartir información personal [5].

En Ecuador desde el año 2019, se ha desarrollado una Ley Orgánica de Protección de Datos Personales, la cual busca crear una legislación especializada que se encargue de regular el tratamiento de datos personales, salvaguarde derechos fundamentales y libertades individuales, promueva la actividad económica y comercial y delimite los parámetros para un tratamiento adecuado de los mismos en el ámbito público y privado [6]. En consecuencia, las empresas deberán ajustar sus procesos, políticas, formas de trabajo e incluso su cultura organizacional, con la finalidad de cumplir con los requerimientos y normativa que la nueva ley impulsará. La ley conmina a las empresas a generar y establecer nuevos perfiles, roles y responsabilidades con la finalidad de que quien tenga acceso y/o control de los datos, lo haga con responsabilidad, con conocimiento de las

implicaciones administrativas, civiles o penales que pueden acarrear el mal uso de los datos.

En este trabajo se propone un marco de trabajo para la aplicación de la ley que permita a empresas grandes y pequeñas conocer el estado de su organización con respecto a la normativa y poder dar los pasos necesarios hacia el cumplimiento de esta. Para lo cual se plantea la utilización de arquitectura empresarial que permita la definición del estado actual y sobre todo el planteamiento del estado futuro de la organización. Este estado final estará determinado por la normativa de protección de datos, para lo cual se plantea la identificación de las mejoras que deben realizar las organizaciones y todos los componentes involucrados dentro de la arquitectura empresarial. Impulsando un cambio a todo nivel en las empresas, lo cual no es nada nuevo en el mundo empresarial, ya que la visión de una empresa estática y estable es un tema lejano y sin validez actual, las empresas actuales están caracterizadas por la evolución e innovación constante, ya sea por factores externos como la economía o las políticas públicas, y por factores internos como nuevos negocios, expansión de mercado o cambios en la tecnología y capacitación de su personal. Para este reto existen varias metodologías, guías y frameworks las cuales adaptan las personas, procesos, tecnología y demás componentes con los cambios. Entre las cuales una de las mayormente usadas, estudiadas y recomendadas es la Arquitectura Empresarial [7], por lo cual se ha decidido en el presente trabajo como base y modelo para identificar los cambios y mejoras que se deben ejecutar de las capas, relaciones y entidades de una organización, para obtener los resultados necesarios de acuerdo con la ley y necesidades de las empresas.

1.1. Objetivo general

Diseñar un marco de trabajo para la identificación y planificación de cambios organizacionales orientados al cumplimiento normativo del Proyecto de Ley Orgánica de Protección de Datos en empresas del Ecuador

1.2. Objetivos específicos

- Realizar una Revisión Sistemática de la Literatura sobre privacidad de información, leyes implementadas, GDPR, arquitectura empresarial y análisis de impacto.

- Analizar la Ley Orgánica de Protección de Datos Personales y sus implicaciones para las empresas con el fin de identificar requerimientos, derechos, prohibiciones y posibles impactos hacia las empresas.
- Diseñar un marco de trabajo que permita a las empresas ejecutar actividades para el cumplimiento de la normativa
- Evaluar el marco de trabajo en dos empresas las cuales han sido seleccionadas por su tamaño y el impacto que puede tener la Ley en sus giros de negocio.

1.3. Marco Teórico

La normativa de protección de datos que mayor impacto y desarrollo ha tenido es la europea, misma que no es nueva tratándose de la preocupación del tratamiento de los datos personales, dado que desde años atrás este continente ha implementado normativas que salvaguarda los datos personales de su población, y que en la actualidad ha ido adecuándose a la nueva realidad social hasta llegar a la publicación del Reglamento General de Protección de Datos, el 27 de abril de 2016 y que fue de obligatorio cumplimiento para los estados miembros a partir del 25 mayo de 2018 (GDPR). El GDPR está diseñado para proteger la privacidad de los ciudadanos europeos incluso sin importar la ubicación de los datos. Según el autor la ley crea grandes beneficios para los ciudadanos, pero se ha convertido en un dolor de cabeza para las organizaciones en cuestiones de cumplimiento y aplicación de la regulación [8].

Por otro lado, existen otras normativas de protección y privacidad de datos las cuales tienen diferencias locales de acuerdo con cada región o país. En una implementación multinacional es importante conocer las normativas vigentes y las diferencias que pueden existir entre cada una de estas. Según D. Baume existen varios factores que influencian las normativas como son las percepciones de privacidad, diferencias en los valores culturales y restricciones legislativas [9].

En Estados Unidos y Canadá la protección y privacidad de datos tienen un alcance y rigurosidad diferente al expresado en el GDPR, caracterizando al modelo estadounidense la autorregulación y existencia de normativa sectorial; y por el momento no existe mayor alineación entre Norte América y la Unión Europea (UE), así el Tribunal de Justicia de la Unión Europea en el asunto C-311/18 — Comisaria de Protección de Datos vs Facebook Irlanda y Maximillian Schrems, consideró que los requisitos del Derecho nacional

estadounidense, y en particular algunos programas que permiten a las autoridades públicas de los Estados Unidos acceder a los datos personales transferidos desde la UE a los EE.UU., con fines de seguridad nacional, imponen limitaciones a la protección de los datos personales que no están circunscritos de un modo que ofrezca garantías sustancialmente equivalentes a las exigidas en el Derecho de la Unión Europea, y que esta legislación no proporciona ninguna vía de recurso judicial contra las autoridades de los Estados Unidos a los titulares de los datos [10].

De hecho, la única jurisdicción norteamericana que ha aprobado un estatuto de protección de datos sobre el modelo europeo es Quebec-Canadá [11]. En ese sentido USA tiene su guía de privacidad basada en la Práctica de Principios de Información Justa (FIP) los cuales incluye: Aviso (conciencia), elección (consentimiento), acceso (participación), integridad (seguridad) y aplicación (reparación). Pero es importante señalar que no existe una completa, única y comprensible normativa de privacidad de datos, existen algunas normativas especializadas como por ejemplo protección de datos de salud o restricción de información de niños y niñas. De hecho, no existe requerimiento legal para los comercios electrónicos para el mantenimiento de políticas de privacidad en USA [9].

En Latinoamérica la protección de datos también ha empezado a ser considerada una prioridad para la regulación y protección de los derechos de las personas; es así como, el primer país en contar con una regulación fue Colombia desarrollando una política pública de explotación de datos, la cual busca la inversión económica para la expansión y uso de datos y la administración de estos como activos que generan valor económico y social. Sin embargo, esto implica la manipulación de datos personales los cuales están protegidos por la Constitución Política de 2008, las cuales están legalmente fundamentadas en el derecho de habeas data [12].

En Brasil el 8 de julio de 2019 fue finalmente aprobada la Ley general de Protección de Datos un estatuto para la regulación del procesamiento de datos, el cual está basado en el GDPR, esta ley entregó un periodo de gracia para implementarla; este periodo finalizó en agosto 2020. Las empresas que violen la ley serán sujetos de aplicación de advertencias, multas, embargos, suspensiones parciales o totales; las multas podrán alcanzar el 2% de los ingresos, con un límite de R$50 millones por violación [13].

Argentina tiene una ley vigente publicada en el año 2000 la cual tiene por objeto la protección integral de los datos personales en donde tiene principios como licitud, calidad,

consentimiento, seguridad, datos de salud, confidencialidad, cesión, transferencia internacional, impugnación entre los principales [14]. Sin embargo, se encuentra en proceso de aprobación de una nueva Ley de Protección de Datos la cual busca alinear la evolución de la tecnología y el impacto que tienen estas con la privacidad de las personas. Adicionalmente al cambio regulatorio que GDPR ejerce en el ámbito internacional [15].

Como se ha podido evidenciar en varios países se está intentando salvaguardar a la privacidad de datos de sus ciudadanos pues a la luz de la actualidad el impacto de la falta de privacidad de datos cada vez gana más terreno en diferentes países y por diferentes medios a través del cual nos desarrollamos. Hay que entender que la privacidad hoy en día es poder y como tesoro preciado debe ser resguardado por cada individuo y garantizado por los estados, la privacidad llega a ser importante porque la falta de ésta da poder a otros sobre cada individuo, poniéndolo en desventaja al existir personas o empresas que saben demasiado provocando como resultado que tengan la facilidad de interferir en la vida de cada uno.

Así menciona Carissa Véliz, profesora de Oxford, que la privacidad debe ser vista como la protección de los abusos de poder sobre un individuo evitando discriminación y debe ser vista como la protección de los abusos de poder sobre la sociedad pues sin está no existen garantías de igualdad, justicia, libertad y democracia, es decir el individuo se vuelve vulnerable a acciones o situaciones discriminatorias que pueden darse en cualquier ámbito de la vida social [16].

Existe también a nivel mundial un alto índice de preocupación por las normativas tanto locales como internacionales. Esto es principalmente por el desconocimiento de las normativas o por lo complicado/ambiguo de las directrices que tiene la normativa e incluso por las mediciones cualitativas que pueden generarse y que a su vez tiene consecuencias sancionatorias bastante rigurosas. También ha obligado a las empresas a tomar mucho más enserio la privacidad de las personas y los procesos de captura, almacenamiento, procesamiento y uso de datos e incluso generaría cambios en los modelos de negocios y la monetización que se realiza con los datos [17].

Por estas razones en el presente trabajo se busca implementar una guía que permita a las empresas clarificar sus dudas sobre la normativa, identificando el estado actual y las actividades donde trabajar y mejorar con el objetivo de generar una correcta implementación de la norma. Tomando en cuenta los cambios y mejoras internas que se

deben ejecutar para conseguir los objetivos de privacidad y protección de datos y así garantizar el cumplimiento de la normativa correspondiente.

1.3.1. Protección de Datos en Ecuador

En Ecuador mediante la Constitución Política de 1998 se incluyó dentro de la sección referente a las garantías de los derechos, la protección de datos y al acceso a los mismos. Estos mecanismos se aplicaban a datos contenidos en documentos o de bancos de datos que se almacenen en entidades públicas o privadas con el objetivo de controlar el uso que se haga de ellos y su propósito. Estas iniciativas se operacionalizaron a través de una figura legal denominada Hábeas Data, el cual constituyó el punto de partida para el propósito de protección de la información personal. De esta manera, se elevó a una categoría de cumplimiento constitucional el derecho de las personas al acceso a documentos, bancos de datos e informes que sobre si mismos o sobre sus bienes consten en entidades públicas y privadas; y para hacerlo debía ser accionada con una petición ante un juez, esta garantía constitucional tenía como espíritu el evitar que se afecte la intimidad de las personas para obtener información de terceros sin autorización de su titular o de autoridad competente [18].

La Constitución de 2008, en su capítulo sexto, aborda con mayor amplitud los Derechos de Libertad, reconociendo y garantizando para todas las personas el derecho a la protección de datos de carácter personal (artículo 66, numeral 19) [19]. Esta protección incluye el acceso y el uso de información personal y datos de este carácter; añadiendo que la recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán de la autorización del titular o por mandato de ley. En este sentido, se ha tratado de implementar normas que sancionen su incumplimiento como el Código Integral Penal, que establece como sanción a la violación a la intimidad una pena privativa de libertad de 1 a 3 años [20]. Sin embargo, no existe una norma específica que regule la protección de datos personales; es decir, no existe una ley específica que lleve a aterrizar, en la práctica, el derecho constitucional de protección de datos. Es así como Ecuador se encuentra en la elaboración y publicación de la Ley Orgánica de Protección de Datos Personales.

Esta ley tiene como objetivo regular el ejercicio del derecho a la protección de datos personales, la autodeterminación informativa y demás derechos digitales en el tratamiento

y flujo de datos personales, a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela.

Los principios que rigen la ley son:

- Juricidad, lealtad y transparencia
- Legitimidad
- Finalidad
- Pertinencia y Minimización de datos personales
- Proporcionalidad del tratamiento
- Consentimiento
- Confidencialidad
- Calidad
- Conservación
- Seguridad de datos personales
- Responsabilidad proactiva y demostrada
- Aplicación favorable al titular
- Independencia de control
- Normativa especializada

De igual manera en la ley se han definido los roles, responsabilidades y derechos que son parte del sistema de protección de datos personales. En donde los principales roles son:

- Titular: Persona natural cuyos datos son objeto de tratamiento.
- Responsable del tratamiento: Persona natural o jurídica, pública o privada, que decide sobre la finalidad y el tratamiento de datos personales.
- Encargado del tratamiento: Persona que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos personales.
- Tercero: Persona que no ostenta la calidad de responsable o encargado de tratamiento; titular; o, Autoridad de Protección de Datos Personales.
- Destinatario: Persona natural o jurídica que ha recibido comunicación de datos personales.
- Autoridad de protección de datos: Entidad de derecho público dependiente de la Función Ejecutiva con personería jurídica y gozará de autonomía administrativa y financiera.
- Entidades certificadoras

- Delegado de protección de datos personales: Cuando existen condiciones especiales como control permanente, información sensible con grandes volúmenes de datos, defensa y seguridad nacional se designará este rol.

Por otro lado, los derechos que el titular de datos personales tiene son:

- Derecho a la lealtad, transparencia e información: El titular de los datos personales tiene el derecho a ser informado de manera leal y transparente. En donde si los datos son obtenidos directamente del titular, la información debe ser comunicada de forma previa o en el momento de la captura de los datos. En caso contrario el titular debe ser informado de manera posterior, dentro del mes siguiente. Esta información debe estar accesible por cualquier medio para garantizar la autorización, tratamiento, transferencia o comunicación de los datos.

- Derecho al acceso: Garantiza acceso a los datos, a conocer cómo son utilizados, y a cualquier información suplementaria que pueda ser utilizada juntos con los datos.

- Derecho a la rectificación y actualización: Otorga el derecho a que sus datos personales sean rectificados en caso de ser incorrectos imprecisos, inexactos, incompletos o falsos.

- Derecho de eliminación: Es el derecho a que sus datos personales sean removidos de cualquier lugar si no existe una razón convincente y justificada para que estén almacenados y que estos no sean tratados por el responsable del tratamiento. Y a su vez el responsable del tratamiento debe implementar métodos y técnicas para eliminar, anular, destruir o hacer ilegible de forma definitiva y segura según la normativa técnica.

- Derecho al olvido digital: Se aplica mediante la solicitud a un juez, la eliminación/ supresión de los datos personales que estén siendo tratados en un entorno digital cuando:
    - Los datos ya no son necesarios para los fines que fueron recogidos.
    - EL interesado retira el consentimiento o solicita su eliminación.
    - El interesado se opone al tratamiento y no existen motivos que prevalezcan para continuar el tratamiento.
    - Los datos fueron tratados de manera ilícita.

    - Los datos son de carácter obsoleto.
    - Los datos no tienen valor histórico o científico.
    - Los datos no tienen relevancia pública.
    - Los datos son inadecuados, impertinentes o excesivos para las fines o tiempo recogido

- Derecho de oposición: Otorga el derecho a objetar o negar el procesamiento de sus datos. Un ejemplo podría ser la objeción de que sus datos sean utilizados por organizaciones de marketing directo o la elaboración de perfiles.

- Derecho de anulación: El titular tiene el derecho a solicitar nulidad por ilicitud en el acto o por tratamiento de datos personales en el ámbito jurisdiccional, bajo las causales de nulidad en materia civil, mercantil o administrativa según sea el caso.

- Derecho a restringir el procesamiento: Permite que sus datos sean almacenados, pero no procesados. Por ejemplo, una persona puede recurrir a este derecho si siente que sus datos erróneos son almacenados a la espera de ser rectificados.

- Derecho a la portabilidad de datos: El titular puede solicitar copias de la información almacenada para utilizar en cualquier otro lugar. Luego de completar la transferencia el responsable inicial que transfirió los datos procederá con la eliminación de los datos del titular.

- Derecho a la limitación del tratamiento: Garantiza el uso mínimo de datos personales en el tratamiento de datos. Incluye la restricción que los datos no se encuentren disponibles en Internet u otros medios, a menos que el acceso sea técnicamente controlado.

- Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas: Permite objetar sobre la toma de decisiones automáticas que se hagan sobre sus datos personales y que produzcan efectos jurídicos o atenten contra sus derechos y libertades. Por ejemplo, la definición de determinados hábitos de compra online, en función a comportamientos previos.
    - Para estos casos el titular podrá:
    - Solicitar explicación sobre la decisión tomada
    - Presentar observaciones.

- Solicitar criterios de valoración sobre el programa automatizado.
- Impugnar la decisión.

Los responsables, encargados del tratamiento de datos personales están sujetos a medidas correctivas, infracciones y sanciones establecidas en la norma. Para lo cual se han clasificado las infracciones en leves y graves; en donde infracciones leves corresponden a tramites fuera de plazo, no notificar a las autoridades de eventos sucedidos de seguridad o privacidad o no tener disponibles políticas de protección de datos e incluso incumplir medidas correctivas. Las sanciones graves constituyen principalmente al mal uso de información personal, no realizar evaluaciones de impacto y riesgo, falta de implementación de protección de datos.

Las sanciones impuestas en la norma para infracciones leves van desde 3% al 9% sobre el volumen del negocio (a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del impuesto sobre el valor agregado y de otros impuestos directamente relacionados con la operación económica), mientras que para infracciones graves la multa tiene un rango del 10% al 17% del volumen del negocio [6].

1.3.2. Arquitectura Empresarial Para la Transformación Empresarial

Una arquitectura empresarial es una descripción de alto nivel destinada a capturar la visión de una empresa que integra todas sus dimensiones: estructura organizativa, procesos empresariales e infraestructura. Cada una de las partes de una empresa está sujeta a cambios, y cada cambio puede tener consecuencias significativas dentro de todos los dominios de la empresa. Por lo tanto, se dedica mucho esfuerzo a mantener la integridad de una descripción arquitectónica [21].

Un cambio importante en las organizaciones a menudo reúne a un grupo diverso de personas que representan a una comunidad de interés y hace que estas se pregunten cómo el cambio les afectará individual y colectivamente. En consecuencia, las estrategias de gestión del cambio deben abordar las necesidades sociológicas y psicológicas del equipo de trabajo. Por lo cual el cambio debe administrarse para que se considere a toda

la organización. Y es aquí donde la arquitectura empresarial juega un papel importante ya que proporciona un enfoque holístico, promueve una comunicación eficaz, integra cultura y la estructura organizacional, reduce la resistencia al cambio y finalmente proporciona un plan de gestión de cambios eficaz [22].

Por ejemplo, en arquitectura empresarial tenemos EA 3 Cube Framework el cual permite enfocar el trabajo para un mejor aprovechamiento de los esfuerzos para la transformación empresarial, promoviendo la colaboración de los interesados tanto en diseño como ejecución de la arquitectura futura (to-be). Este marco de arquitectura empresarial permite la correlación de una vista jerárquica tradicional de la empresa a un modelo que promueve e integra los componentes estratégicos, comerciales y tecnológicos que caracterizan a las organizaciones grandes y complejas [22].

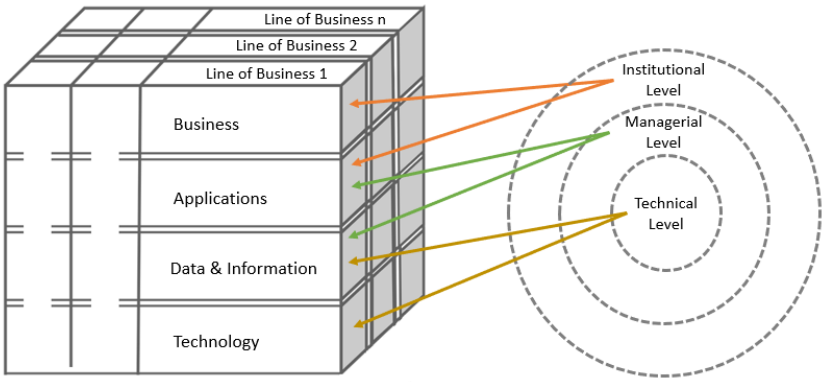


Figura 1: Relación del modelo organizacional y arquitectura empresarial

Tomando ese análisis del impacto y relación entre los dominios de la arquitectura empresarial, la estructura jerárquica de una empresa, y la interrelación que existen en sus componentes, se definen los dominios que impactan la empresa para el cumplimiento de la normativa. Estos dominios están agrupados en función de los requerimientos de la norma y basados en la arquitectura empresarial. Permitiendo una mejor identificación del impacto, cambios y controles que se deben implementar en la organización. Esta relación está definida en la Figura 2, en donde se han planteado 5 nuevos dominios que envuelven la protección de datos desde todos sus ángulos y que se detallan en la siguiente sección. Estos dominios de protección de datos son:

- Políticas
- Estructura Organizacional
- Seguridad

- Transferencia y Comunicación
- Datos

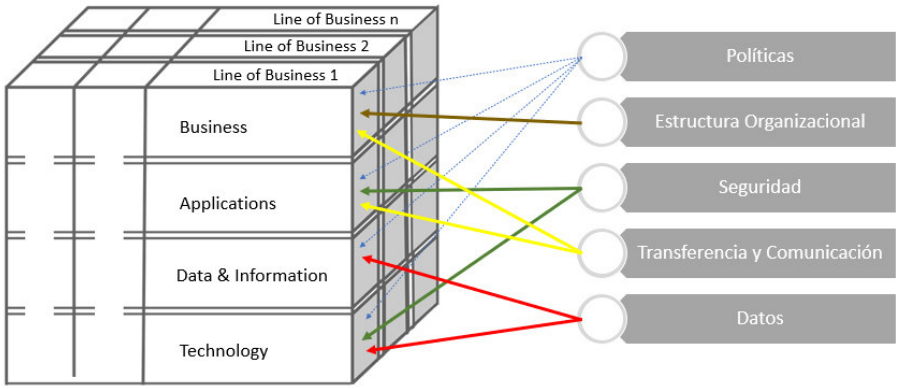


Figura 2: Mapeo de arquitectura empresarial y dominios de protección de datos personales

2. METODOLOGÍA

Para el presente trabajo se utilizó la metodología de Ciencia del Diseño (Design Science Research) para la creación de un marco de trabajo para las empresas que sirva de acompañamiento en el proyecto de ley de protección de datos en el Ecuador. La Ciencia del Diseño se ocupa de la creación y/o transformación de objetos artificiales para resolver problemas teóricos o prácticos. Los artefactos pueden ser materiales o inmateriales, incluyendo sus modalidades de interacción con los ambientes socio técnicos y culturales en los que se insertan [23].

El objetivo final de Ciencia del Diseño es proveer un modelo mental con las características buscadas en la investigación, para lo cual se incluyen los siguientes seis pasos (Figura 3):

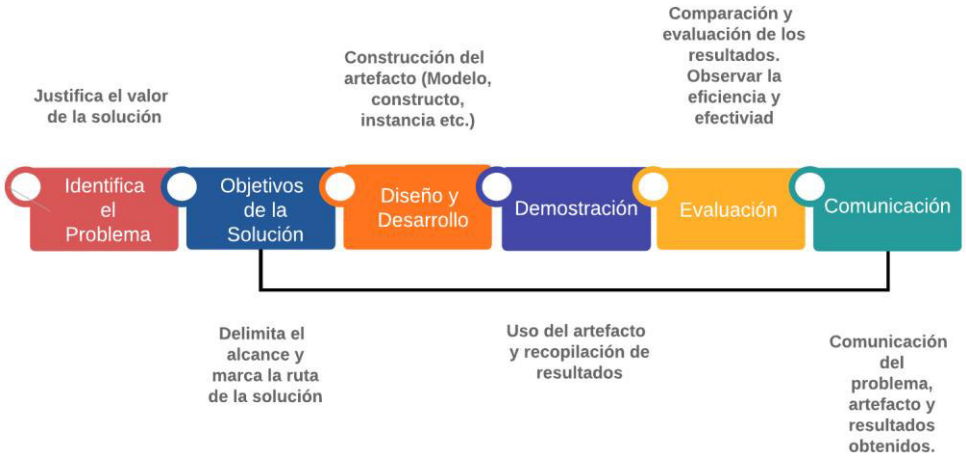


Figura 3: Pasos de Ciencias del Diseño

- Identificar el problema: Definir el problema de investigación específico y justificar el valor de una solución. Dado que la definición del problema se utilizará para desarrollar un artefacto que pueda proporcionar una solución de manera efectiva, es útil atomizar el problema conceptualmente para que la solución pueda capturar su complejidad. Justificar el valor de una solución logra dos cosas: motiva al investigador y a la audiencia parapara buscar la solución y aceptar los resultados, y ayuda a comprender el razonamiento asociado con la comprensión del problema por parte del investigador. Los recursos necesarios para esta actividad incluyen el conocimiento del estado del problema y la importancia de su solución.

- Definir objetivos de la solución: Inferir los objetivos de una solución a partir de la definición del problema y el conocimiento de lo que es posible y factible. Los objetivos pueden ser cuantitativos o cualitativos. Los objetivos deben inferirse

racionalmente de la especificación del problema. Los recursos necesarios para ello incluyen el conocimiento del estado de los problemas y las soluciones actuales, si las hay, y su eficacia.

- Diseño & desarrollo: Crea el artefacto. Tales artefactos son potencialmente construcciones, modelos, métodos o instanciaciones. Conceptualmente, un artefacto de investigación de diseño puede ser cualquier objeto diseñado en el que se incrusta una contribución de investigación en el diseño. Esta actividad incluye determinar la funcionalidad deseada del artefacto y su arquitectura y luego crear el artefacto real. Los recursos necesarios para pasar de los objetivos al diseño y desarrollo incluyen el conocimiento de la teoría que se puede aplicar en una solución.

- Demostración: Se demuestre la utilidad del artefacto para resolver una o más instancias del problema. Esto podría involucrar su uso en experimentación, simulación, estudio de caso, prueba u otra actividad apropiada. Los recursos necesarios para la demostración incluyen un conocimiento efectivo de cómo usar el artefacto para resolver el problema.

- Evaluación: Observe y mida qué tan bien el artefacto apoya una solución al problema. Esta actividad implica comparar los objetivos de una solución con los resultados reales observados del uso del artefacto en la demostración. Requiere conocimiento de métricas relevantes y técnicas de análisis. Dependiendo de la naturaleza del lugar del problema y del artefacto, la evaluación puede tomar muchas formas. Podría incluir elementos como una comparación de la funcionalidad del artefacto con los objetivos de la solución de la actividad dos anterior, medidas de desempeño cuantitativas objetivas, como presupuestos o elementos producidos, los resultados de encuestas de satisfacción, comentarios de los clientes o simulaciones. Podría incluir medidas cuantificables del rendimiento del sistema, como el tiempo de respuesta o la disponibilidad. Conceptualmente, dicha evaluación podría incluir cualquier evidencia empírica o prueba lógica apropiada. Al final de esta actividad, los investigadores pueden decidir si volver al paso tres para tratar de mejorar la eficacia del artefacto o continuar con la comunicación y dejar las mejoras para los proyectos posteriores. La naturaleza del lugar de la investigación puede determinar si dicha iteración es factible o no.

- Comunicación: Comunicar el problema y su importancia, el artefacto, su utilidad y novedad, el rigor de su diseño y su efectividad a los investigadores y otras audiencias relevantes, como los profesionales en ejercicio, cuando sea apropiado. En las publicaciones de investigación académica, los investigadores pueden utilizar la estructura de este proceso para estructurar el artículo, al igual que la estructura nominal de un proceso de investigación empírica (definición del problema, revisión de la literatura, desarrollo de hipótesis, recopilación de datos, análisis, resultados, discusión y conclusión). es una estructura común para trabajos de investigación empírica. La comunicación requiere conocimiento de la cultura disciplinaria [24].

2.1. Marco de Trabajo

Se propone la creación y aplicación de un marco de trabajo como mecanismo de ayuda y de una guía para la implementación efectiva de la normativa de Protección de datos en el Ecuador, también permite la evaluación del estado actual de las organizaciones en referencia a lo esperado por la norma. Ver Figura 4

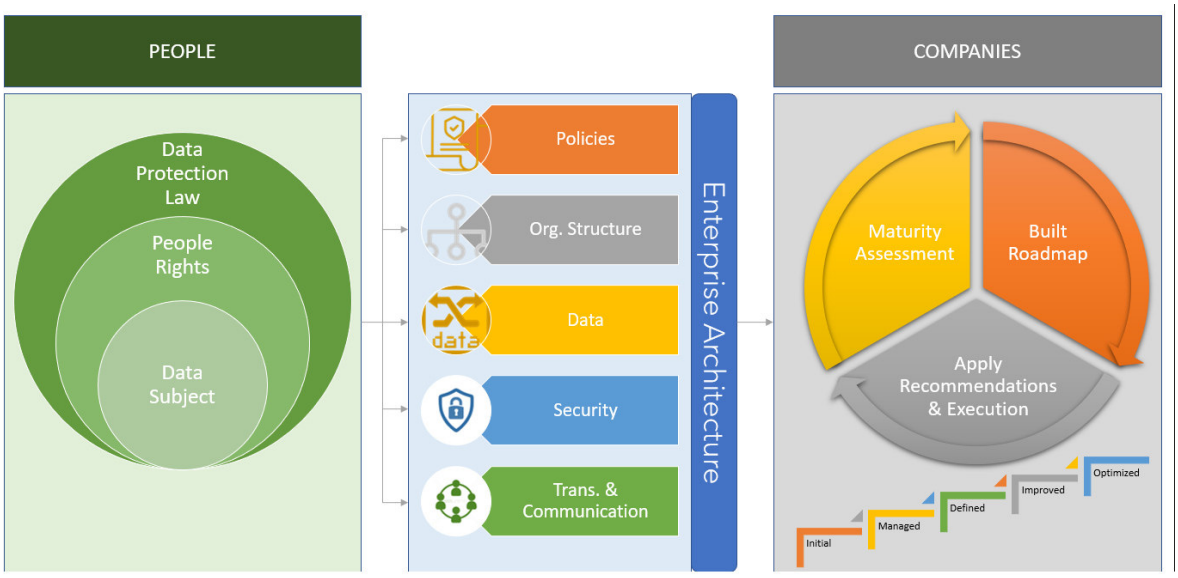


Figura 4: Marco de Trabajo

En Figura 5 se detallan los dominios que deben tomarse en cuenta para la aplicación del marco de trabajo en donde los factores de cumplimiento son Políticas, Datos, Seguridad, Estructura Organizacional y Transferencia y Comunicación.

Figura 5: Factores de Cumplimiento del Marco de Trabajo

A continuación, se detallan cada uno de los dominios:

Políticas: Incluye las políticas y estándares en torno a la privacidad de información de datos personales. Los niveles de madurez se basan en la creación y formalización de políticas y normas de gestión de la información, luego por adopción plena y la incorporación a la estructura básica de una organización.

Datos: Administración de datos contempla tener las herramientas, prácticas y procedimientos con el fin de establecer y mantener los datos con adecuada calidad. Es el estado de integridad, validez, coherencia, oportunidad y precisión que hace que los datos apropiados para un uso específico.

Seguridad: Información sobre seguridad y privacidad busca entender cómo hace la empresa con la protección de los datos e información como un activo vital. La seguridad tiene que ver con la capacidad de proteger la información y los datos, la privacidad tiene que ver con quién está autorizado a ver qué activo. Vinculando estos conceptos se busca incorporar la seguridad desde el diseño.

Estructura Organizacional: Los niveles de madurez de conciencia organizacional del Gobierno de Información se establecen por el nivel de trabajo en equipo entre el negocio y TI. Una fuerte conciencia sobre el valor de los datos y los riesgos en torno a que los datos

se vuelven más prominentes y crea estructuras de control eficaces que permitan medir la persistencia y el perfeccionamiento de gobierno en toda la empresa.

Transferencia y Comunicación: Permite ejecutar de manera ordenada, organizada y segura la información de los titulares hacia un tercero a nivel nacional o internacional. Sin olvidar la importancia que tiene la comunicación con los sujetos de datos en los procesos de la organización sean o no vinculados a procesos con datos personales.

El cumplimiento de la normativa debe ser evaluado para lo cual, como parte del marco de trabajo se aplica una encuesta que permite la identificación del nivel de madurez de la organización con respecto a la protección de datos personales y a su vez identifica la brecha de acuerdo con las necesidades de cada organización. Para permitir esta evaluación se propone una escala numérica de cinco (5) posibles respuestas en donde cada etapa representa una mejora sustancial de las capacidades de protección de datos personales, los niveles son:

- Inicial: No existen procesos que velen por la protección de datos personales, existen iniciativas individuales mas no colectivas de la organización.
- Administrado: Gestión básica de protección de datos, no existe disciplina en el cumplimiento de procesos y políticas de protección de datos.
- Definido: Conjunto de procesos estándar que se utilizan para establecer coherencia en toda la organización.
- Mejorado: Procesos bien definidos y que tienen mediciones cuantitativas y cualitativas de los indicadores clave de rendimiento (KPI) definidos para la protección de datos personales.
- Optimizado: Revisión continua de los indicadores, los cuales se encuentran completamente vinculados a los procesos del negocio. Participación constante de los responsables de protección de datos.

Con esta forma de evaluación en cada uno de los dominios podemos identificar el estado actual (as is) de la organización y también definir el estado deseado (to be) tomando en cuenta que se debe llegar al cumplimiento total en todos los dominios para un correcto cumplimiento de la normativa de protección de datos, pero cada empresa puede priorizar los pasos a dar teniendo estados intermedios de implementación de acuerdo con su giro de negocio y necesidades organizacionales. Para lo cual es importante reconocer que cada paso hacia adelante nos permite llegar a los objetivos planteados, pero estos requieren de

tiempo, recursos y dedicación para alcanzarlos, por lo cual es recomendable identificar los dominios en los que queremos trabajar basados en un plan o en la planificación estratégica de la organización para priorizar las actividades en función de necesidades puntuales.

Una vez compiladas las encuestas identificaremos los dominios en los cuales tenemos mayor brecha de acuerdo con los objetivos de cada organización ver Figura 6.

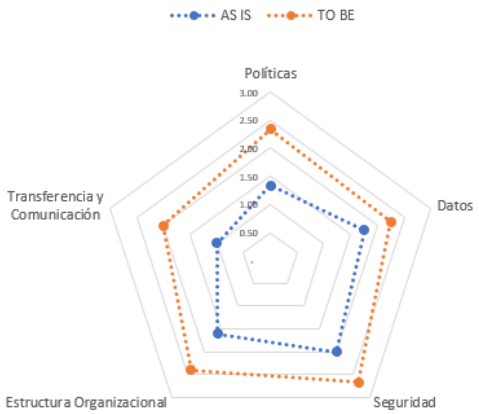


Figura 6: Brecha de Protección de Datos Personales

Finalmente, como parte del marco de trabajo propuesto se pueden revisar las actividades y controles recomendados que nos permitirán pasar a los siguientes niveles, estos controles también tienen la identificación del impacto en la arquitectura empresarial en donde pueden existir afectaciones ya sea en tecnología, aplicaciones, datos y/o negocio. Con lo cual se tiene un cuadro completo de las necesidades de protección de datos personales, que controles se deben aplicar para cubrir dichas necesidades y cuál es el impacto en la arquitectura empresarial de la implementación de esos controles.

3. RESULTADOS Y DISCUSIÓN

A continuación, se presenta la aplicación del marco de trabajo para protección de datos personales según la normativa ecuatoriana, se ha realizado la evaluación a dos empresas privadas, para mayor detalle revisar los Anexos I, II, III, IV.

La empresa A en la cual se aplicó el marco de trabajo es una empresa dedicada a la venta de seguros de personas naturales con especialización en seguros de vida y accidentes personales. Cuenta con más de 25 años en el mercado ecuatoriano.

Fundamentados en esa misión de cumplir con sus clientes y preocupados por la creciente demanda de protección de datos en el país, se decide aplicar el marco de trabajo para protección de datos personales.

Se inició con el involucramiento de una de las gerencias para poder tener el respaldo necesario al interno de la organización, ya que es importante el reconocimiento de esta necesidad a un nivel gerencial. Se realizó la respectiva evaluación para identificar el estado actual de la organización de acuerdo con los dominios o factores de cumplimiento del marco de trabajo. Los resultados obtenidos se muestran en la Tabla 1.

DOMINIOS	AS IS	TO BE	Variación
Políticas	1,33	2,33	75%
Datos	1,75	2,25	29%
Seguridad	1,80	2,50	39%
Estructura Organizacional	1,60	2,40	50%
Transferencia y Comunicación	1,00	2,00	100%

Tabla 1: Resultados Encuesta Empresa A

En donde se tiene una mayor perspectiva de crecimiento es en los dominios de Políticas y Transferencia – Comunicación ya que se evidenció la necesidad de fortalecer tanto las políticas internas como los procesos y procedimientos que realicen manipulación de datos personales y sobre todo trabajar en la captura y administración adecuada del consentimiento de parte del titular de los datos, ya que sin esta autorización todos los demás procesos no pueden ser ejecutados de manera adecuada. De igual manera la transferencia y comunicación de las medidas de control, políticas y procesos deben ser correctamente evaluadas con los proveedores o externos para garantizar una adecuada administración de la información personal. En los otros dominios se bien existen mejoras

que se deben realizar son menores que las antes descritas, por ejemplo, en seguridad el cual es el dominio mejor calificado ya que se vienen varios años trabajando en este ámbito siempre existen mejoras que realizar, llevando a la organización a mejores niveles de conciencia e importancia de la seguridad en términos de privacidad, confidencialidad y disponibilidad.

En resumen, el primer paso que se va a implementar es la administración del consentimiento del titular de datos mediante el cual se garantiza la posibilidad de tratar, procesar y almacenar los datos personales. Y la creación de un rol que tome el control de la protección de datos personales para la emisión de directrices que permitan una apropiada y oportuna generación de controles y protección de datos personales.

La segunda aplicación del marco de trabajo se realizó para la empresa B. la cual tiene una amplia trayectoria en el análisis de datos y manejo de información para generar ventajas competitivas en diferentes organizaciones mediante la aplicación de consultorías especializadas.

En esta aplicación se pudo evidenciar un diferente enfoque en las características y necesidades de la organización, ya que, a diferencia de la anterior aplicación, en la empresa B la principal preocupación de los directivos es garantizar una adecuada transferencia de datos, desde el responsable de los datos hasta la empresa B, quien será el tercero en es este proceso de analítica de datos. Los resultados obtenidos están en la Figura 7.

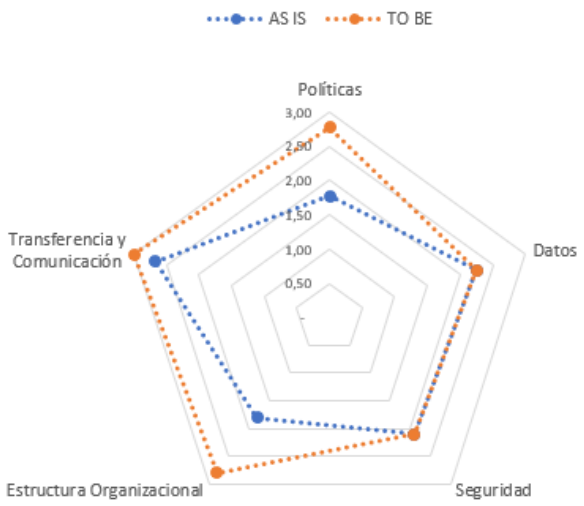


Figura 7: Brecha en Encuesta Empresa B

En este caso se priorizaron los dominios de Estructura organizacional, Políticas y Transferencia - Comunicación los cuales según las necesidades identificadas por el negocio y la actividad a la que se dedica, y a su vez no se ha planificado tener crecimiento en los dominios de Seguridad y Datos (Ver Tabla 2) ya que en años pasados han trabajado en estos dominios; enfocados en establecer una buena base de cara a los requerimientos de tanto organizaciones como entidades de control se han priorizado los dominios que permitan establecer normas, procesos, políticas que apoye las actividades y genere confianza a sus clientes. Y que esto a su vez genere una ventaja competitiva con el cumplimiento de esta normativa y apalancando una mejor reputación en el mercado. Por lo cual se ha planificado un proceso donde la seguridad y privacidad sean tomadas desde el inicio en cada uno de los procesos.

DOMINIOS	AS IS	TO BE	Variación
Políticas	1,78	2,78	56%
Datos	2,25	2,25	0%
Seguridad	2,10	2,10	0%
Estructura Organizacional	1,80	2,80	56%
Transferencia y Comunicación	2,67	3,00	13%

Tabla 2: Resultados Encuesta Empresa B

4. CONCLUSIONES

- El proyecto de Ley Orgánica de Protección de Datos Personales dejo de ser proyecto y se convirtió en Ley Orgánica de obligatorio cumplimiento para las empresas del sector público como del privado con su publicación en el Registro Oficial No. 459 de 26 de mayo de 2021, con la finalidad de garantizar el ejercicio del derecho a la protección de datos personales.

- La publicación de la Ley Orgánica de Datos Personales viabiliza de manera práctica la protección de los datos personales como el derecho fundamental consagrado en la Constitución de la Republica del Ecuador

- La ley Orgánica de Protección de Datos Personales ecuatoriana, plantea grandes retos que deben satisfacer las empresas privadas y las del sector público, para lo cual deberán en un plazo de 2 años implementar medidas jurídicas, técnicas y organizativas encaminadas a salvaguardar los datos entregados por los ciudadanos, en el desarrollo de actividades que involucren la recolección, procesamiento, archivo y cualquier tipo de tratamiento que se realice con dichos datos.

- La Ley Orgánica de Protección de Datos Personales otorga a los ciudadanos, titulares de datos, derechos para exigir límites en el uso de la información, es decir le atribuye el poder de controlar y disponer de sus datos personales y el uso que se tiene de ellos por parte de terceros.

- El marco de trabajo elaborado implementa disposiciones de la ley y utiliza arquitectura empresarial para la definición del estado actual y los pasos hacia el cumplimiento de la norma en las empresas.

- El marco de trabajo permite una guía de evaluación e implementación en el camino de la protección de datos personales por cuanto permite definir un mapa de ruta para el cumplimiento de la ley de una manera evolutiva y ordenada, admitiendo una priorización de las actividades en función de la estrategia organizacional.

- El marco de trabajo se aplicó en dos empresas, la primera en una empresa dedicada a la venta y comercialización de seguros y la segunda en una firma consultora especializada en temas de análisis de datos. Al utilizar el marco propuesto, ambas empresas conocieron el estado de su organización con respecto a la normativa e identificaron los pasos a seguir para una correcta aplicación de la normativa.

- La aplicación del marco de trabajo en las dos empresas permitió definir los estados intermedios y enfocar sus recursos y tiempo para cumplir con sus prioridades de negocio, como también alineó su planificación estratégica al cumplimiento de la Ley.

- Los gerentes y directores están cada vez más involucrados y conscientes de la información y los datos de sus organizaciones, conociendo el impacto sancionatorio que puede tener el incumplimiento.

- Las empresas deben alinear sus iniciativas y objetivos con la estrategia comercial de cada una de las organizaciones para la obtención de buenos resultados, así en los casos de implementación se pudo notar que, la primera empresa busca repotenciar políticas, reglas, procesos de privacidad, a través de la seguridad y la estructura organizacional; sin embargo, la Compañía B alineada con su facturación busca mejorar no solo las políticas y procesos de su negocio, sino también la protección de datos confiados por clientes por ser transferidos y comunicados por terceros al ser proveedores de servicios analíticos.

- Una Ley Orgánica en el Ecuador es un primer paso hacia este objetivo, que debe evolucionar con el apoyo tanto de la ciudadanía como de las organizaciones públicas y privadas para asegurar una adecuada implementación, que garantice estos derechos fundamentales de las personas.

REFERENCIAS BIBLIOGRÁFICAS

[1] D. Kim, K. Park, Y. Park, and J. H. Ahn, “Willingness to provide personal information: Perspective of privacy calculus in IoT services,” *Comput. Human Behav.*, vol. 92, pp. 273–281, 2019, doi: 10.1016/j.chb.2018.11.022.

[2] R. D. Atkinson and D. Castro, “Digital Quality of Life: Understanding the Personal and Social Benefits of the Information Technology Revolution,” *SSRN Electron. J.*, no. October, 2011, doi: 10.2139/ssrn.1278185.

[3] K. N. Uche M. Mbanaso, Centre for Cyberspace, Nasarawa State University, “Personal Data Privacy and Security - Who , What , When , Why , Where and How ?,” *DIRISA Natl. Res. Data Work. Pretoria South Africa*, no. June, pp. 1–8, 2018.

[4] G. Fawkes, “Report: Ecuadorian Breach Reveals Sensitive Personal Data,” *VpnMentor*, 2019. https://www.vpnmentor.com/blog/report-ecuador-leak/ (accessed Apr. 07, 2020).

[5] P. F. Drucker, *Technology, management and society*. 2012.

[6] Asamblea Nacional del Ecuador, “Proyecto de Ley Orgánica de Protección de Datos Personales.” Quito, 2019, [Online]. Available: www.asambleanacional.gob.ec.

[7] N. Saboya Ríos, O. L. Loaiza Jara, and D. Lévano Rodríguez, “Diseño de un modelo de arquitectura empresarial para publicaciones científicas basado en ADM - TOGAF 9.0,” *Apunt. Univ.*, vol. 8, no. 1, pp. 52–67, 2018, doi: 10.17162/au.v8i1.186.

[8] S. Sirur, J. R. C. Nurse, and H. Webb, “Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR),” *Proc. ACM Conf. Comput. Commun. Secur.*, no. iii, pp. 88–95, 2018, doi: 10.1145/3267357.3267368.

[9] D. L. Baumer, J. B. Earp, and J. C. Poindexter, “Internet privacy law: A comparison between the United States and the European Union,” *Comput. Secur.*, vol. 23, no. 5, pp. 400–412, 2004, doi: 10.1016/j.cose.2003.11.001.

[10] E. Members, “Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311 / 18 — Comisaria de Protección de Datos vs Facebook Irlanda y Maximillian Schrems,” pp. 1–6, 2020.

[11] C. J. Bennett and C. D. Raab, “The adequacy of privacy: The european union data protection directive and the north american response,” *Inf. Soc.*, vol. 13, no. 3, pp. 245–264, 1997, doi: 10.1080/019722497129124.

[12] J. Silva, D. Solano, C. Fernandez, L. Romero, and J. V. Villa, “Privacy preserving, protection of personal data, and big data: A review of the Colombia case,” *Procedia Comput. Sci.*, vol. 151, no. 2018, pp. 1213–1218, 2019, doi:

10.1016/j.procs.2019.04.174.

[13] R. Koch, “What is the LGPD? Brazil’s version of the GDPR,” 2019. https://gdpr.eu/gdpr-vs-lgpd/ (accessed Jul. 25, 2020).

[14] R. Pascual, J. Genoud, and G. Aramburu, “PROTECCION DE LOS DATOS ARGENTINA,” 2000. http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm (accessed Jul. 25, 2020).

[15] Dirección Nacional de Protección de Datos Argentina, *Cuadro Comparativo*. 2020, p. 28.

[16] I. Hernández Velasco, “Carissa Véliz, profesora de Oxford: ‘La falta de privacidad ha causado, indirectamente, más muertes que el terrorismo,’” 2020. https://www.bbc.com/mundo/noticias-54476232.

[17] S. Ziegler, “Digital business models: Driving transformation and innovation,” *Digit. Bus. Model. Driv. Transform. Innov.*, pp. 201–226, 2018, doi: 10.1007/978-3-319-96902-2.

[18] Asamblea Nacional Constituyente, *Constitución Política De La República del Ecuador, 1998*, vol. 1998, no. 000. Ecuador, 1998, p. 94.

[19] C. L. y de F. Asamblea Nacional del Ecuador, *Constitución de la República del Ecuador*. Ecuador, 2008, pp. 32–34.

[20] Asamblea Nacional, “Código Orgánico Integral Penal- Ley 0,” *Editor. Nac.*, p. 144, 2014.

[21] F. S. De Boer, M. M. Bonsangue, L. P. J. Groenewegen, A. W. Stam, S. Stevens, and L. Van Der Torre, “Change impact analysis of enterprise architectures,” *Proc. 2005 IEEE Int. Conf. Inf. Reuse Integr. IRI - 2005*, vol. 2005, pp. 177–181, 2005, doi: 10.1109/IRI-05.2005.1506470.

[22] F. Espinoza, “Enterprise architecture and change management,” *J. Enterp. Archit.*, vol. 3, no. 2, pp. 27–35, 2007, doi: 10.1080/15459624.2013.818222.

[23] R. Baskerville, J. Pries-Heje, and J. Venable, “Soft design science methodology,” *Proc. 4th Int. Conf. Des. Sci. Res. Inf. Syst. Technol. DESRIST ’09*, 2009, doi: 10.1145/1555619.1555631.

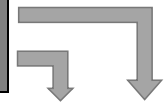
[24] S. Editors, *Integrated Series in Information Systems*. .

ANEXOS

Anexo I – Evaluación de Madurez Empresa A

EVALUACIÓN DE MADUREZ PROTECCIÓN DE DATOS PERSONALES

1 - Inicial: No existen procesos que velen por la protección de datos personales, existen iniciativas individuales mas no colectivas de la organización.
2 - Administrado: Gestión básica de protección de datos, no existe disciplina en el cumplimiento de procesos y políticas de protección de datos.
3 - Definido: Conjunto de procesos estándar que se utilizan para establecer coherencia en toda la organización.
4 - Mejorado: Procesos bien definidos y que tienen mediciones cuantitativas y cualitativas de los kpi definidos para la protección de datos personales.
5 - Optimizado: Revisión continua de los indicadores, los cuales se encuentran completamente vinculados a los procesos del negocio. Participación constante de los responsables de protección de datos.



	AS IS	TO BE
Políticas Incluye las políticas y estándares en torno a la privacidad de información de datos personales. Los niveles de madurez se basan en la creación y formalización de políticas y normas de gestión de la información, luego por adopción plena y la incorporación a la estructura básica de una organización.	1,33	2,33
P1. Actualmente hay políticas básicas implementadas para la administración de los datos personales en la empresa.	1	2
P2. Las revisiones y actualizaciones a las políticas y procedimientos de datos personales son evidentes.	1	2
P3. Políticas de datos personales se construyen en colaboración de todos o varios departamentos.	1	2
P4. La política de datos personales esta relacionada directamente con el consentimiento, eliminación, actualización, olvido digital y la confidencialidad de los usuarios finales	1	2
P5. Las nuevas políticas de datos personales o los cambios a una política existente, se lleva a cabo en un proceso sistemático y con un responsable definido.	3	3
P6. Las políticas de datos personales se integran con la empresa y/o Políticas Operativas para la mejora continua.	2	3
P7. El consentimiento de las personas finales es tratado como un habilitante principal, sin el cual no continúan los demás procesos como tratamiento, almacenamiento o transferencia de datos	1	3
P8. Existen mecanismos que permitan al titular de datos administrar (acceder, visualizar, eliminar y actualizar) la información entregada.	1	2
P9. ¿Son los usuarios finales (titular) comunicados oportunamente del uso y tratamiento que se dan de sus datos?	1	2

Datos Administración datos significa tener las herramientas, prácticas y procedimientos con el fin de establecer y mantener los datos con adecuada calidad. Es el estado de integridad, validez, coherencia, oportunidad y precisión que hace que los datos apropiados para un uso específico. Incluye la administración de datos y sus respectivas categorías, para poder aplicar medidas de seguridad, calidad, confidencialidad específicas a los datos personales.	1,75	2,25
D1. Se ha implementado procesos de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.	2	2
D2. Existen procesos de mitigación de riesgos como respaldos, control de accesos, roles y permisos para la administración de datos personales	3	3
D3. Para datos sensibles ya sean estos historial médico, datos de menores de edad, fallecidos u otros. Existen medidas de seguridad y privacidad específicas que permitan mantener la protección de sus titulares.	1	2
D4. Para la eliminación de datos existen métodos de anonimización de datos que garanticen la imposibilidad de identificación del titular.	1	2

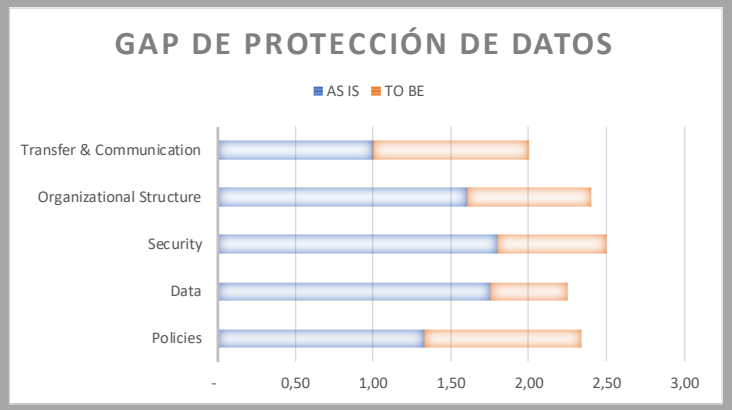
Seguridad		
Información sobre seguridad y privacidad busca entender cómo hace la empresa con la protección de los datos e información como un activo vital. La seguridad tiene que ver con la capacidad de proteger la información y los datos, la privacidad tiene que ver con quién está autorizado a ver qué. El conjunto de preguntas a continuación ayuda a facilitar una comprensión de la madurez de la organización para hacer frente a ambos problemas	1,80	2,50
S1. La administración es consciente de la conservación de la información personal en los sistemas informáticos y los datos relacionados con la legislación de estos.	3	3
S2. Existen algunas herramientas para hacer cumplir las políticas de seguridad de los datos en la mayoría de los sistemas.	1	2
S3. Los accesos de los empleados se controla / restringe de acuerdo a roles específicos, "autorizados" de la información.	3	3
S4. La Seguridad de la Información se considera tanto en la transmisiones de datos para / cliente / proveedor personal sobre la red (s).	1	2
S5. Políticas específicas, prácticas o procedimientos se utilizan para asegurar la información sensible del personal (PHI)	2	3
S6. Se han establecido sistemas para predecir las brechas de seguridad y privacidad y resolverlos proactivamente antes de la ocurrencia	1	2
S7. El nivel de Seguridad y privacidad de elementos de datos cifrados se aplican de manera coherente en toda la empresa.	3	3
S8. Se han llevado a cabo evaluación de impacto del tratamiento de datos personales.	2	2
S9. Existen procesos definidos de notificación a entes de control cuando se sufran vulneraciones a los datos personales.	1	2
S10. Existe una metodología formal que incluye el análisis, desarrollo en regla, implementación y prueba de la calidad y seguridad de datos	1	3

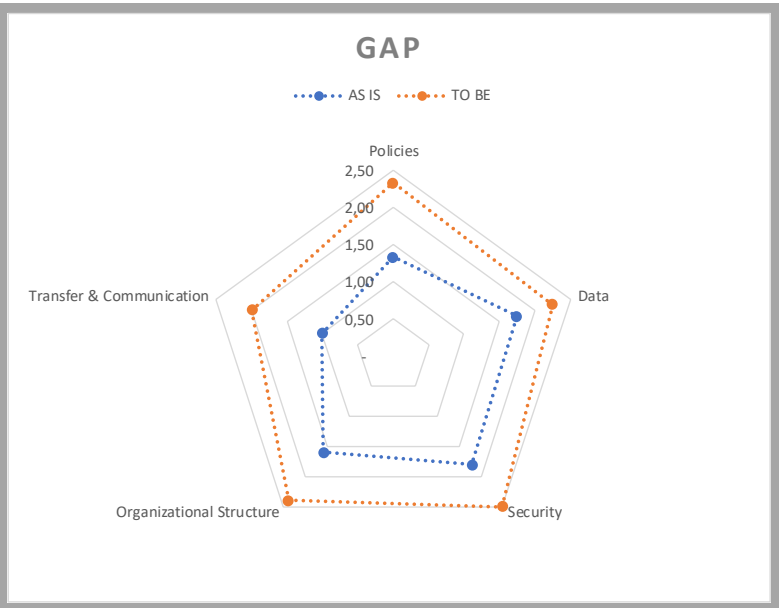
Estructura Organizacional		
Los niveles de madurez de conciencia organizacional de Información de Gobierno se establecen por el nivel de trabajo en equipo entre el negocio y TI. Una fuerte conciencia sobre el valor de los datos y los riesgos en torno a que los datos se vuelven más prominentes y crea estructuras de control eficaces que permitan medir la persistencia y el perfeccionamiento de las conductas de gobierno en toda la empresa.	1,6	2,4
E1. Hay algunas políticas y prácticas ejecutándose para el uso de los datos dentro de la Empresa.	1	2
E2. Existe una conciencia creciente acerca de la importancia de los datos, su aporte a la empresa y la responsabilidad de proteger los datos	3	3
E3. Hay un plan escrito sobre cómo los datos y la información se gestiona dentro de la Empresa.	2	3
E4. Existe un delegado de protección de datos personales en la empresa	1	2
E5. Existe participación activa de parte del responsable de protección de datos personales en las decisiones de la compañía	1	2

Transferencia y Comunicación		
Permite ejecutar de manera ordenada, organizada y segura la información de los titulares hacia un tercero a nivel nacional o internacional	1,00	2,00
T1. Existen procedimientos definidos para la transferencia de datos personales a terceros?	1	2
T2. Para enviar información a otra entidad existen evaluaciones de privacidad y seguridad de datos previo al envío	1	2
T3. Se realizan contratos de responsabilidad que permitan realizar la transferencia y custodia adecuada de los datos personales	1	2

Anexo II – Resultados de la Evaluación en Empresa A

DOMAINS	AS IS	TO BE	VARIATION
Policies	1,33	2,33	75%
Data	1,75	2,25	29%
Security	1,80	2,50	39%
Organizational Structure	1,60	2,40	50%
Transfer & Communication	1,00	2,00	100%





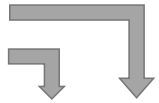
Recomendaciones

Políticas	Incluye las políticas y estándares en torno a la privacidad de información de datos personales. Los niveles de madurez se basan en la creación y formalización de políticas y normas de gestión de la información, luego por adopción plena y la incorporación a la estructura básica de una organización.	Ver Detalle
Datos	Administración de datos significa tener las herramientas, prácticas y procedimientos con el fin de establecer y mantener los datos con adecuada calidad. Es el estado de integridad, validez, coherencia, oportunidad y precisión que hace que los datos apropiados para un uso específico.	Ver Detalle
Seguridad	Información sobre seguridad y privacidad busca entender cómo hace la empresa con la protección de los datos e información como un activo vital. La seguridad tiene que ver con la capacidad de proteger la información y los datos, la privacidad tiene que ver con quién está autorizado a ver qué activo.	Ver Detalle
Estructura Organizacional	Los niveles de madurez de conciencia organizacional de Información de Gobierno se establecen por el nivel de trabajo en equipo entre el negocio y TI. Una fuerte conciencia sobre el valor de los datos y los riesgos en torno a que los datos se vuelven más prominentes y crea estructuras de control eficaces que permitan medir la persistencia y el perfeccionamiento de gobierno en toda la empresa.	Ver Detalle
Transferencia y Comunicación	Permite ejecutar de manera ordenada, organizada y segura la información de los titulares hacia un tercero a nivel nacional o internacional	Ver Detalle

Anexo III – Evaluación de Madurez Empresa B

EVALUACIÓN DE MADUREZ PROTECCIÓN DE DATOS PERSONALES

1 - Inicial: No existen procesos que velen por la protección de datos personales, existen iniciativas individuales mas no colectivas de la organización.
2 - Administrado: Gestión básica de protección de datos, no existe disciplina en el cumplimiento de procesos y políticas de protección de datos.
3 - Definido: Conjunto de procesos estándar que se utilizan para establecer coherencia en toda la organización.
4 - Mejorado: Procesos bien definidos y que tienen mediciones cuantitativas y cualitativas de los kpi definidos para la protección de datos personales.
5 - Optimizado: Revisión continua de los indicadores, los cuales se encuentran completamente vinculados a los procesos del negocio. Participación constante de los responsables de protección de datos.



	AS IS	TO BE
Políticas Incluye las políticas y estándares en torno a la privacidad de información de datos personales. Los niveles de madurez se basan en la creación y formalización de políticas y normas de gestión de la información, luego por adopción plena y la incorporación a la estructura básica de una organización.	1,78	2,78
P1. Actualmente hay políticas básicas implementadas para la administración de los datos personales en la empresa.	2	3
P2. Las revisiones y actualizaciones a las políticas y procedimientos de datos personales son evidentes.	1	2
P3. Políticas de datos personales se construyen en colaboración de todos o varios departamentos.	2	3
P4. La política de datos personales esta relacionada directamente con el consentimiento, eliminación, actualización, olvido digital y la confidencialidad de los usuarios finales	1	2
P5. Las nuevas políticas de datos personales o los cambios a una política existente, se lleva a cabo en un proceso sistemático y con un responsable definido.	2	3
P6. Las políticas de datos personales se integran con la empresa y/o Políticas Operativas para la mejora continua.	2	3
P7. El consentimiento de las personas finales es tratado como un habilitante principal, sin el cual no continúan los demás procesos como tratamiento, almacenamiento o transferencia de datos	2	3
P8. Existen mecanismos que permitan al titular de datos administrar (acceder, visualizar, eliminar y actualizar) la información entregada.	3	4
P9. ¿Son los usuarios finales (titular) comunicados oportunamente del uso y tratamiento que se dan de sus datos?	1	2

Datos Administración datos significa tener las herramientas, prácticas y procedimientos con el fin de establecer y mantener los datos con adecuada calidad. Es el estado de integridad, validez, coherencia, oportunidad y precisión que hace que los datos apropiados para un uso específico. Incluye la administración de datos y sus respectivas categorías, para poder aplicar medidas de seguridad, calidad, confidencialidad específicas a los datos personales.	2,25	2,25
D1. Se ha implementado procesos de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.	2	2
D2. Existen procesos de mitigación de riesgos como respaldos, control de accesos, roles y permisos para la administración de datos personales	3	3
D3. Para datos sensibles ya sean estos historial médico, datos de menores de edad, fallecidos u otros. Existen medidas de seguridad y privacidad específicas que permitan mantener la protección de sus titulares.	3	3
D4. Para la eliminación de datos existen métodos de anonimización de datos que garanticen la imposibilidad de identificación del titular.	1	1

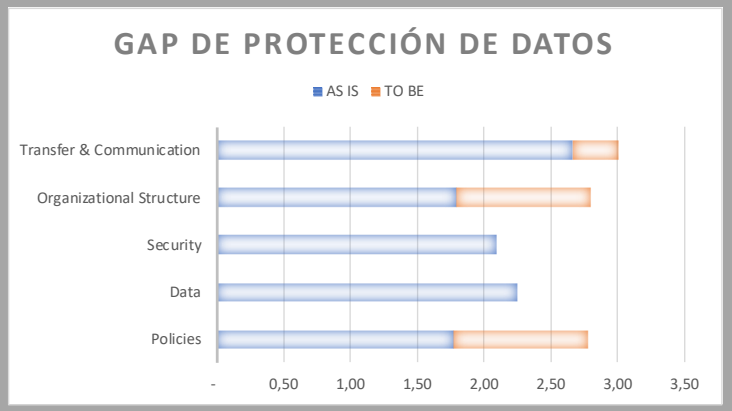
Seguridad		
Información sobre seguridad y privacidad busca entender cómo hace la empresa con la protección de los datos e información como un activo vital. La seguridad tiene que ver con la capacidad de proteger la información y los datos, la privacidad tiene que ver con quién está autorizado a ver qué. El conjunto de preguntas a continuación ayuda a facilitar una comprensión de la madurez de la organización para hacer frente a ambos problemas	2,10	2,10
S1. La administración es consciente de la conservación de la información personal en los sistemas informáticos y los datos relacionados con la legislación de estos.	3	3
S2. Existen algunas herramientas para hacer cumplir las políticas de seguridad de los datos en la mayoría de los sistemas.	3	3
S3. Los accesos de los empleados se controla / restringe de acuerdo a roles específicos, "autorizados" de la información.	3	3
S4. La Seguridad de la Información se considera tanto en la transmisiones de datos para / cliente / proveedor personal sobre la red (s).	2	2
S5. Políticas específicas, prácticas o procedimientos se utilizan para asegurar la información sensible del personal (PHI)	2	2
S6. Se han establecido sistemas para predecir las brechas de seguridad y privacidad y resolverlos proactivamente antes de la ocurrencia	2	2
S7. El nivel de Seguridad y privacidad de elementos de datos cifrados se aplican de manera coherente en toda la empresa.	1	1
S8. Se han llevado a cabo evaluación de impacto del tratamiento de datos personales.	2	2
S9. Existen procesos definidos de notificación a entes de control cuando se sufran vulneraciones a los datos personales.	1	1
S10. Existe una metodología formal que incluye el análisis, desarrollo en regla, implementación y prueba de la calidad y seguridad de datos	2	2

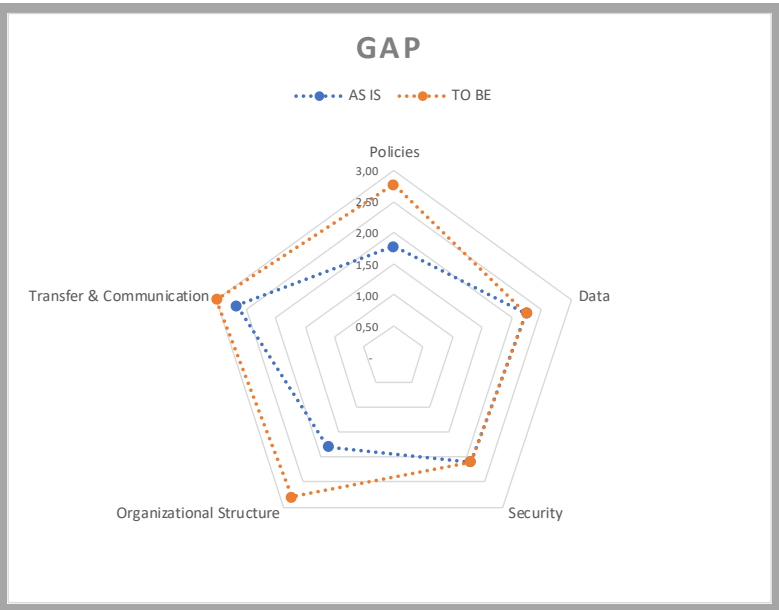
Estructura Organizacional		
Los niveles de madurez de conciencia organizacional de Información de Gobierno se establecen por el nivel de trabajo en equipo entre el negocio y TI. Una fuerte conciencia sobre el valor de los datos y los riesgos en torno a que los datos se vuelven más prominentes y crea estructuras de control eficaces que permitan medir la persistencia y el perfeccionamiento de las conductas de gobierno en toda la empresa.	1,8	2,8
E1. Hay algunas políticas y prácticas ejecutándose para el uso de los datos dentro de la Empresa.	2	3
E2. Existe una conciencia creciente acerca de la importancia de los datos, su aporte a la empresa y la responsabilidad de proteger los datos	3	4
E3. Hay un plan escrito sobre cómo los datos y la información se gestiona dentro de la Empresa.	2	3
E4. Existe un delegado de protección de datos personales en la empresa	1	2
E5. Existe participación activa de parte del responsable de protección de datos personales en las decisiones de la compañía	1	2

Transferencia y Comunicación		
Permite ejecutar de manera ordenada, organizada y segura la información de los titulares hacia un tercero a nivel nacional o internacional	2,67	3,00
T1. Existen procedimientos definidos para la transferencia de datos personales a terceros?	3	3
T2. Para enviar información a otra entidad existen evaluaciones de privacidad y seguridad de datos previo al envío	2	3
T3. Se realizan contratos de responsabilidad que permitan realizar la transferencia y custodia adecuada de los datos personales	3	3

Anexo IV – Resultados de la Evaluación en Empresa B

DOMAINS	AS IS	TO BE	VARIATION
Policies	1,78	2,78	56%
Data	2,25	2,25	0%
Security	2,10	2,10	0%
Organizational Structure	1,80	2,80	56%
Transfer & Communication	2,67	3,00	13%





Recomendaciones

Políticas	Incluye las políticas y estándares en torno a la privacidad de información de datos personales. Los niveles de madurez se basan en la creación y formalización de políticas y normas de gestión de la información, luego por adopción plena y la incorporación a la estructura básica de una organización.	Ver Detalle
Datos	Administración de datos significa tener las herramientas, prácticas y procedimientos con el fin de establecer y mantener los datos con adecuada calidad. Es el estado de integridad, validez, coherencia, oportunidad y precisión que hace que los datos apropiados para un uso específico.	Ver Detalle
Seguridad	Información sobre seguridad y privacidad busca entender cómo hace la empresa con la protección de los datos e información como un activo vital. La seguridad tiene que ver con la capacidad de proteger la información y los datos, la privacidad tiene que ver con quién está autorizado a ver qué activo.	Ver Detalle
Estructura Organizacional	Los niveles de madurez de conciencia organizacional de Información de Gobierno se establecen por el nivel de trabajo en equipo entre el negocio y TI. Una fuerte conciencia sobre el valor de los datos y los riesgos en torno a que los datos se vuelven más prominentes y crea estructuras de control eficaces que permitan medir la persistencia y el perfeccionamiento de gobierno en toda la empresa.	Ver Detalle
Transferencia y Comunicación	Permite ejecutar de manera ordenada, organizada y segura la información de los titulares hacia un tercero a nivel nacional o internacional	Ver Detalle