

Case report / Reporte de caso / Relato de caso - Tipo 5

# Law on Transparency implementation process, ISO 27001 and Database Reporting on public entities

**Ing. Edward Fabián Penagos Granada** / efpenagos@gmail.com

**Msc. Ana María López Echeverry** / anamayi@utp.edu.co

**Msc. Paula Andrea Villa Sánchez** / pavaji@utp.edu.co

Grupo de investigación Telecomunicaciones – Nyquist. Universidad Tecnológica de Pereira, Colombia

**ABSTRACT** During 2015 and 2016, in Pereira (Colombia) a training project addressed to public entities officials was carried out in areas related with: law on transparency, ISO 27001 and database reporting, through theoretical and practical sessions. As a result, a local researching group developed a set of documents with relevant and updated information on each topic. So, officials can use them as implementation guides in their respective institutions. This paper describes how the training sessions was developed. Finally, the results of the project are presented in a positive way, taking as a reference both an initial scenario and final scenario of greater complexity.

**KEYWORDS** Training; law on transparency; ISO 27001; information security; database reporting.

Proceso de implementación de la ley de transparencia, la ISO 27001 y el reporte de base de datos en entidades públicas

**RESUMEN** Durante 2015 y 2016, en la ciudad de Pereira se adelantó un proyecto de capacitación para los funcionarios de varias entidades públicas de la ciudad en temas relacionados con la ley de transparencia, la ISO 27001 y el reporte de bases de datos, a través de sesiones teórico-prácticas. Fruto de ese proyecto, un grupo de investigación de la región realizó investigaciones para entregar un conjunto de documentos con información actualizada y pertinente de cada temática, para que estos funcionarios puedan utilizarlas como guías de implementación en sus respectivas instituciones. En este documento se describe cómo se crearon y desarrollaron las sesiones de capacitación y se presentan los resultados del proyecto, positivos, tomando como referencia un escenario inicial y un escenario final, de mayor complejidad.

**PALABRAS CLAVE** Capacitación; ley de transparencia; ISO 27001; seguridad de la información; reporte de base de datos.

Processo de implementação da lei de transparência, da ISO 27001 e do relatório de bancos de dados em entidades públicas

**RESUMO** Durante 2015 e 2016, foi desenvolvido na cidade de Pereira, um projeto de formação para os funcionários de várias organizações públicas da cidade sobre questões relacionadas com a lei da transparência, a ISO 27001 e o relatório de bancos, mediante sessões teórico-práticas. Como resultado deste projeto, um grupo de investigação na região realizou pesquisas para entregar um conjunto de documentos com informações atualizadas e relevantes de cada tema, de forma que os funcionários possam usá-las como guias de implementação em suas respectivas instituições. Este documento descreve como foram criadas e desenvolvidas as sessões de formação e apresenta resultados do projeto, positivos, com referência a uma fase inicial e uma fase final, de maior complexidade.

**PALAVRAS-CHAVE** Formação; lei de transparência; ISO 27001; segurança de informação; relatório de bancos de dados.

## I. Introduction

With the purpose of understanding the objective of the project and the research developed, it is necessary to indicate that in the call No. 705-2015 of Colciencias, the aim is to strengthen innovation nodes in areas such as (IT Architecture, Cyber Security, Health and Citizen Services). In order to contribute to the increase of productivity and the Information and Communication Technologies [ICT] sector competitiveness, also to bring research activity closer to industry and to strengthen public administration. As a result, it was developed the project “Training Online Government Security, Law on Transparency and Databases Reporting Colciencias 538”

The project is focused on three specific ways: The first one is approached to achieve the knowledge right through the access to the public information, since as Newman (2015) indicates, this right is constituted in a citizen tool to make transparent all the institutions that receive and manage the resources of the state, and thus guarantee by this exposure to the public, citizens take actions aimed at demanding their accountability. The second one is aimed to reach an effective database reporting process, which protects the integrity, confidentiality and availability of information, since the protection of personal data is a fundamental right that seeks to defend the rights of holders, such as intimacy, honor, moral integrity and life - in the late 1940s this topic was already being discussed in the world. However, due to technological development and the emergence of new forms of information, it has been necessary to rethink its scope and content-. The third one to attain the implementation of the online government strategy, which seeks to ensure that companies belong to the public sector, specifically territorial and national entities, comply with the components “Security and privacy of information”, in accordance with The stipulated deadlines In Decree 2573 of 2014, with which “... the general guidelines of the Online Government Strategy are established, Law 1341 of 2009 is partially regulated and other provisions are given.”. Working hand in hand with the international standard ISO 27001.

On the other hand, in order to achieve the commitments of these themes, not only in terms of indicators, but also of effectiveness and implementation in public entities; it is necessary to have a population trained to act and entities and officials trained to serve; Thus, this project expect to train officials, through the development of specific contents and studies prepared for each of the research topics, with the support of pedagogical methodologies and, at the same time, virtual environments such as a virtual learning platform configuration case.

## I. Introducción

Para entender cuál es el objetivo del proyecto y del trabajo realizado, es preciso indicar que en la convocatoria No. 705-2015 de Colciencias se busca fortalecer los nodos de innovación en temas como (Arquitectura de TI, Ciberseguridad, Salud y Servicios al Ciudadano) con el fin de contribuir al incremento de la productividad y de la competitividad del sector de las Tecnologías de la Información y las Comunicaciones [TIC], acercar la actividad investigativa a la industria y fortalecer la administración pública. Por esta razón surge el proyecto “Capacitación seguridad gobierno en línea, ley de transparencia y reporte de bases de datos Colciencias 538”

El proyecto se centra en tres líneas específicas: la primera va enfocada a garantizar el derecho al saber a través del acceso a la información pública, ya que como lo indica Newman (2015), este derecho se constituye en una herramienta ciudadana para transparentar a todas aquellas instituciones que reciban, gestionen o administren recursos del estado (sujetos obligados), y garantiza así que, por esta exposición al público, la ciudadanía tome acciones encaminadas a exigir la rendición de cuentas por parte de estos; la segunda va orientada a lograr un proceso de reporte de bases de datos efectivo, que proteja la integridad, confidencialidad y disponibilidad de la información, ya que la protección de datos personales es un derecho fundamental que busca defender los derechos de los titulares, como la intimidad, el honor, la integridad moral y la vida —desde finales de los años 40 ya se hablaba de este tema en el mundo, pero debido al desarrollo tecnológico y a la aparición de nuevas formas de compartir información, ha sido necesario replantear su alcance y contenido—; la tercera lograr la implementación de la estrategia gobierno en línea, la cual busca que las empresas del sector público, específicamente las entidades del orden territorial y nacional, den cumplimiento al componente “Seguridad y privacidad de la información”, de acuerdo con los plazos estipulados en el Decreto 2573 de 2014, con el cual “... se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.”, tarea para cuyo logro se ha venido trabajando de la mano con la norma internacional ISO 27001.

Por otra parte, para cumplir con lo propuesto en estas temáticas, no solo en términos de indicadores, sino también de efectividad e implementación en las entidades públicas, es necesario contar con una población capacitada para actuar y unas entidades y funcionarios capacitados para servir; así, este proyecto busca formar y capacitar a funcionarios, a través del desarrollo de contenidos específicos y casos prácticos para cada uno de los temas de investigación, con el apoyo de metodologías pedagógicas y, al mismo tiempo, haciendo uso de ambientes virtuales como es el caso de la configuración de una plataforma de aprendizaje virtual.

Para poder implementar las políticas y los modelos definidos por el gobierno en materia de seguridad, se requiere contar con un grupo base debidamente formado que esté en capacidad de liderar los procesos de cambio organizacional necesarios para dar cumplimiento a las políticas definidas, como son aspectos de seguridad de Gobierno en Línea, Ley de transparencia y reporte de bases de datos. Durante el desarrollo del proyecto se estableció una línea base del conocimiento de los funcionarios de las instituciones participantes acerca de estas temáticas, la que permitió definir un plan de formación con ejemplos prácticos dirigidos a elevar el nivel de conocimiento en las instituciones y dejarlas preparadas para emprender un proceso de implementación.

## II. Metodología

En primera instancia se realizó un proceso de consulta de bibliografía y documentos relacionados con cada temática, luego se construyó el posible contenido general de la temática para la capacitación de los funcionarios públicos –que fue revisado y aprobado por una empresa consultora externa experta en los temas–. Una vez aprobado el contenido general, se desarrollaron los contenidos específicos. Antes de iniciar el curso de formación se aplicó una encuesta a los funcionarios sobre la temática en cuestión para medir el grado de conocimiento, en estos temas, determinar debilidades y fortalezas, y encaminar de la mejor manera la orientación de los cursos.

Como se mencionó, la ciudadanía y los funcionarios deben capacitarse para garantizar el cumplimiento efectivo de la ley de transparencia (ley 1712 de 2014), el reporte de base de datos (Decreto 886 de 2014) y la ISO 27001, por lo tanto, se realizó un análisis de las metodologías de aprendizaje que debían tenerse en cuenta durante el proceso de formación, para que los funcionarios asimilaran el conocimiento de la mejor manera, a través del establecimiento de un plan de formación con ejemplos prácticos.

Para atender estas necesidades de formación se utilizaron como metodologías la pedagogía de la problematización, metodología que basa su aprendizaje en la interpretación del entorno y en la identificación de problemas sociales que requieran una investigación para su óptima solución (Delgado, 2009); y el Modelo Didáctico Operativo [MDO], el cual propone el diseño y desarrollo de experiencias de aprendizaje a través de la producción y aplicación del conocimiento, como metodología de aprendizaje.

Con estos modelos pedagógicos, se procedió a generar unas guías de apoyo para su implementación, las cuales poseían una estructura que cubre: el conocimiento de la ley, norma o decreto; el conocimiento histórico y normativo; y la implementación. A continuación se presenta una descripción de cada uno de los ejes temáticos presentes en el proyecto.

In order to implement the policies and models defined by the government in terms of security, it is necessary to have a duly formed core group, capable of leading the processes of organizational change to achieve the policies, such as aspects of Online Government Security, Law on Transparency and Database Reporting. During the development of the project, a baseline of the officials knowledge belongs to the participating institutions was established. As a result, it was allowed to define a training plan with practical examples aimed at raising the level of knowledge in institutions and leave them prepared to undertake an implementation process.

## II. Methodology

In a first instance, a process of bibliography session and documents related to each theme was carried out. Then, a possible general content for the civil servants training was created. reviewed and approved by an external consulting firm. Once the general content was approved, the specific contents were developed. Before starting the training course, a survey was carried out on each subject, with the purpose of assessment the degree of knowledge in the areas mentioned above, identification of weaknesses and strengths, and guidance of the courses through the best way.

As mentioned above, citizens and officials should be trained to ensure the effectiveness of the Transparency (Law 1712 of 2014), the Database Reporting (Decree 886 of 2014) and ISO 27001. Therefore, it was made an analysis of the learning methodologies that should be taken into account during the training process, hence the employees assimilate knowledge in the best way, through the creation of a training plan with functional examples.

In order to attend these training needs, it was used the pedagogy of problematization as methodology. It is based on the environment interpretation and social problems identification, which require a research for its optimal solution (Delgado, 2009); And the Operational Didactic Model [MDO], which proposes the design and development of learning experiences through the production and application of knowledge, as a learning methodology.

With these pedagogical models, support guides were developed for their implementation, which had a structure that covered: knowledge of the law, rule or decree; historical and normative knowledge; and implementation. Subsequently is a description of each of the thematic axes belonging to the project.

### A. Law 1712 of 2014 or law on transparency and public information access right

#### *Characterization process*

Law 1712 was designed to benefit civil society, independent of its socio-economic conditions. Thus, the first task was focused on recognizing and identifying the particularities - characteristics, needs, interests, expectations and preferences of citizens, users or stakeholders with whom they interact with a person, in order to group them by similarities.

To obtain the information used in this chapter, several guides were used, including:

- “Methodological Guide for the Formulation of Indicators” (DNP, 2009);
- “Guide for citizens, users and interest groups characterization” (DNP, 2011); and
- “Guide for users of public entities characterization” (MinTIC, 2011).

However, these documents are not the same, the similarities and creating a single chapter for the characterization process, along with a detailed procedure aimed at finding those needs (**TABLE 1**), where each of the tabs (green color) has an implementation aspect.

#### *Information management tools*

Once the characterization procedure was defined, information management tools were developed. They allow identifying, classifying and publishing the information under control or custody of an obligated subject. Thus, it could be available to citizens who require it.

When the alliance called “More Information, More Rights” (2014) began to promote the Law on Transparency and access to public information in Colombia, taking as reference framework the “Model Inter-American Law on Access to Public Information” (OAS, 2010), It was determined that the tools for information management would be one of its main provisions. These instruments are: the Information assets registration; the classified and confidential information index; the Information publication scheme; and the document management program. It should be notified that although these instruments have similar fields (as will be seen), they cannot be kept in a single file, as they are required by law separately.

Given the importance of these instruments for a successful implementation of Law 1712, several chapters were developed to the understanding and creation of these instruments mentioned above.

### A. Ley 1712 de 2014 o ley de transparencia y del derecho de acceso a la información pública

#### *Proceso de caracterización*

La ley 1712 de 2014 fue pensada para beneficiar a la sociedad civil, independiente de sus condiciones socio-económicas. Así, la primera tarea desarrollada se enfocó en reconocer e identificar las particularidades –características, necesidades, intereses, expectativas y preferencias– de los ciudadanos, usuarios o interesados con los cuales interactúa una entidad, con el fin de agruparlos por similitudes.

Para obtener la información utilizada en este capítulo, se utilizaron varias guías, entre ellas:

- la “Guía metodológica para la formulación de indicadores” (DNP, 2009);
- la “Guía de caracterización de ciudadanos, usuarios y grupos de interés” (DNP, 2014); y
- la “Guía para la caracterización de usuarios de las entidades públicas” (MinTIC, 2011).

No obstante, estos documentos no son iguales, por ello, se optó por realizar una extracción de las similitudes y la creación de un solo capítulo para el proceso de caracterización, junto con un procedimiento detallado dirigido a encontrar dichas necesidades (**TABLA 1**), donde cada una de las pestañas (color verde) tiene un aspecto de la implementación.

#### *Instrumentos para la gestión de la información*

Una vez definido el procedimiento de caracterización, se procedió a construir los instrumentos para la gestión de la información, los cuales sirven para identificar, clasificar y publicar la información que se encuentra en posesión, bajo control o en custodia de un sujeto obligado; así, estos puedan tenerla disponible para los ciudadanos que la requieran.

Cuando la alianza “Más información más derechos” (2014) comenzó a promover la ley de transparencia y acceso a la información pública en Colombia, teniendo como marco de referencia la “Ley modelo interamericana sobre acceso a la información pública” (OEA, 2010), se determinó que los instrumentos para la gestión de la información serían una de sus principales disposiciones. Estos instrumentos son: el registro de activos de información; el índice de información clasificada y reservada; el esquema de publicación de información; y el programa de gestión documental. Cabe anotar que, aunque estos instrumentos tienen campos similares (como se verá), no se pueden tener en un solo archivo, ya que por ley se requieren por separado.

Dada la importancia que tienen estos instrumentos para una implementación exitosa de la Ley 1712, se desarrollaron varios capítulos dedicados a la comprensión y creación de estos.

Para la construcción de los tres primeros instrumentos se comenzó a trabajar en una plantilla creada por los autores de este documento basada en la documentación presente

Table 1. Procedure themes to create a characterization process / Procedimiento para realizar un proceso de caracterización

Documento de soporte para la implementación de la ley 1712 de 2014.	
Procedure Name <i>/Nombre del procedimiento</i>	Characterization procedure conception / <i>Concepción del procedimiento de caracterización.</i>
Objective <i>/Objetivo</i>	This procedure offers a guide to generate a characterization procedure. It is a tool to identify particularities (characteristics, needs, interests, expectative, and preferences) of the citizens, users or stakeholders with whom they interact with a person, in order to group them by similarities. Subsequently, it is necessary to design processes in order to satisfy those needs. This procedure is an important requirement to enforce the Law 1712 of 2014 / <i>Este procedimiento tiene como finalidad ofrecer una guía para la realización de un proceso de caracterización que sirve como herramienta para identificar las particularidades (características, necesidades, intereses, expectativas y preferencias) de los ciudadanos, usuarios o interesados, con los cuales interactúa una entidad, con el fin de agruparlos, según atributos o variables similares, y posteriormente diseñar los procesos de tal manera que se satisfagan dichas necesidades. Este procedimiento es un requisito indispensable para darle cumplimiento a la ley 1712 de 2014 y a sus decretos reglamentarios.</i>
Content <i>/Contenido</i>	This document contains seven tabs (see lines below) to enforce the Law 1712 / 2014 and regulatory decrees 103 and 1081 of 2015 / <i>Este documento cuenta con siete pestañas que permiten darle cumplimiento a la ley 1712 de 2014 y los decretos reglamentarios 103 y 1081 de 2015 (líneas siguientes).</i>
Law-decrees compliance <i>/Cumplimiento ley-decretos</i>	This tab contains information related with the articles in order to achieve both the Law 1712 of 2014 as regulatory decrees (Decree 103 and 1081 of 2015), in addition to the documentation and procedures to accomplish each article / <i>Esta pestaña contiene información relacionada con los artículos a los cuales se da cumplimiento, tanto a la ley 1712 de 2014, como a sus decretos reglamentarios (103 y 1081 de 2015), así como a la documentación y los procedimientos asociados para darle cumplimiento a cada uno de estos artículos.</i>
Start characterization <i>/Inicio caracterización</i>	This tab is an instructive that allows identifying particularities (characteristics, needs, interests, expectative, and preferences) of the citizens, users or stakeholders / <i>Esta pestaña es un instructivo para identificar las particularidades (características, necesidades, intereses, expectativas y preferencias) de los ciudadanos, usuarios o interesados.</i>
Leading team <i>/Equipo líder</i>	This tab is used to identify an interdisciplinary working group that leads the characterization coordinates inside of the entity with the others interested in the information usage / <i>Esta pestaña sirve para identificar una dependencia o un grupo de trabajo interdisciplinario que lidere el ejercicio de caracterización y coordine al interior de la entidad con las dependencias interesadas en el uso de la información.</i>
Variables analysis <i>/Análisis de variables</i>	This part of the characterization process allows identifying which kind of variables should be studied and which is the level of disintegration of the information required. Once the variables have been identified of measurement during the characterization, it is necessary to prioritize, in order to choose the most important variables that allow achieving the objectives / <i>Este segmento sirve para identificar cuáles son los tipos de variables o categorías que se deberán estudiar y cuál es el nivel de profundidad o desagregación de la información requerido. Una vez identificadas las variables a medir en el ejercicio de caracterización es importante hacer una priorización de las mismas, con el fin de escoger solamente aquellas que sean relevantes para el cumplimiento de los objetivos.</i>
Information collection <i>/Recolectar información</i>	This tab indicates how to identify the mechanisms to collect the information that will be used as supply to make a characterization to citizens, users or stakeholders. It is necessary to establish the scope, resources and review the objectives of the characterization / <i>En esta pestaña se indica cómo se deben identificar los mecanismos mediante los cuales se puede recolectar la información que servirá como insumo para la caracterización de los ciudadanos, usuarios o interesados; es muy importante establecer el alcance, los recursos y nuevamente repasar los objetivos del ejercicio de caracterización, ya que éstos determinarán los instrumentos que se deben utilizar.</i>
Segments sets <i>/Establecer segmentos</i>	This tab pretends to reach the database automation that facilitates the analysis, crossing and filter information in order to assemble the citizens, users or stakeholders / <i>El objetivo de esta pestaña es lograr la estructuración y automatización de bases de datos que faciliten el análisis, cruce y filtro de la información, con el fin de agrupar a los ciudadanos, usuarios o interesados, según características similares.</i>
Information publication <i>/ Publicar información</i>	This tab allows making an internal information disclosure process. So, the results can be known by the entities and others. Therefore, the decision making and the design of interventions could be easier / <i>En esta pestaña se pretende realizar un proceso interno de divulgación de la información, para que los resultados sean conocidos por todas las dependencias y los responsables de procesos y servicios, y así facilitar y mejorar la toma de decisiones y el diseño de las intervenciones.</i>
Procedure's update <i>/ Actualización del procedimiento</i>	This procedure does not have to be updated. It should be made completely when a law requires to be implemented, and also when it is wanted to have the best impact to the society / <i>Este procedimiento no se actualiza, por el contrario, este debe realizarse completamente cuando se vaya a implementar una nueva ley y se desea tener el mejor impacto sobre la sociedad.</i>

In order to the construction of the first three instruments, the study began on a template created by the authors of this study. It was based on current documentation from the portals web of some agencies and state pages that have already advanced on the law implementation, Such as the Transparency Secretariat and the Attorney General's Office. As a result of this study, support files were generated in Excel, which was used as support tools for the instruments understanding and as an input for their creation inside the entities.

The fields in "Information asset registration" instrument are: Item; category; information name; information description; language; support tool; format; information available; and published information.

The fields in "Classified and discreet information index" instrument are: Item; category; information name; language; support tool; information creation date; information creation stakeholder name; Information stakeholder name; Exception legitimate object; type; exception legitimate object; description; constitutional or legal basis.

The fields in "Information publication scheme fields" instrument are: Item; information name; language; support tool; format; information creation date; update frequency; office (consulting place); information stakeholder name; information stakeholder

The development of the information publication scheme required more work since its integration with the Government's online program strategy was necessary. It allowed the construction of a dedicated section along with a File, developed in MS-Excel. It contains the minimum publishable information that must be submitted by an obligated subject, which can be used as a self-evaluator or as compliance indicator. Furthermore, delving into the study of the Online Government program it was required to design a quick guide for open data publication from a non-technical point of view, in order to be understood by officials who do not have a profile related to the areas of Systems or similar.

*Document Management Program [DMP]*

The DMP, according to the General Archive of the Nation (2014), is a planning instrument that must be taken into account for the basic operation of a territorial entity. So, the planning, processing, management and Organization of the information generated by the entity can be defined.

To begin the instrument construction, an analysis of the entity was proposed in order to diagnose the state of its document management and to identify its weaknesses and strengths, based on citizen and organization needs in Relation to

en los portales web de algunos organismos y en páginas del Estado que ya han adelantado trabajos en la implementación de la ley, tales como los de la Secretaría de Transparencia y la Procuraduría General de la Nación. Fruto de este trabajo se generaron unos archivos de soporte en Excel, que servían como herramientas de apoyo para la comprensión de los instrumentos y como insumo para su creación al interior de las entidades.

Los campos presentes en el instrumento "Registro de activos de información" son: ítem; categorías o series; nombre o título de la información; descripción de la información; idioma; medio de conservación y/o soporte; formato; e información (disponible / publicable).

Los campos presentes en el instrumento "Índice de información clasificada y reservada" son: ítem; categorías o series; nombre o título de la información; idioma; medio de conservación y/o soporte; fecha de generación de la información; nombre del responsable de producción de la información; nombre del responsable de la información; objeto legítimo de la excepción (tipo y descripción); fundamento constitucional o legal; fundamento jurídico de la excepción; excepción total o parcial; fecha de la calificación; y plazo de la calificación o reserva.

Los campos presentes en el instrumento "Esquema de publicación" son: : ítem; nombre o título de la información; idioma; medio de conservación y/o soporte; formato; fecha de generación de la información; frecuencia de actualización; lugar de consulta; responsable de la producción de la información; y responsable de la información.

El desarrollo del esquema de publicación de la información requirió de mayor trabajo dado que era necesaria su integración con la estrategia de publicación del programa de Gobierno en Línea, lo cual condujo a la construcción de una sección dedicada a dicho programa, junto con un archivo, desarrollado en MS-Excel que contiene la información mínima publicable que debe entregar un sujeto obligado. Este último puede ser utilizado como auto-evaluador o como indicador de cumplimiento. Asimismo, al profundizar en el programa Gobierno en Línea surgió la necesidad de diseñar una guía rápida para la publicación de datos abiertos desde un enfoque no técnico, con el objetivo de que fuese fácilmente comprendido por los funcionarios que no tengan un perfil relacionado con las áreas de sistemas o afines.

*Programa de gestión documental [PGD]*

El PGD, de acuerdo con el Archivo General de la Nación (2014), es un instrumento de planeación que debe ser tenido en cuenta para el funcionamiento básico de una entidad territorial, para que defina la planeación, el procesamiento, el manejo y la organización documental de toda la información producida o recibida por la entidad.

Para comenzar la construcción de este instrumento se propuso realizar un análisis de la entidad, con el fin de diagnosticar el estado de su gestión documental e identifi-

car así cuáles son sus debilidades y fortalezas, con base en las necesidades de la ciudadanía y de la organización en relación con las solicitudes de acceso a la información. El siguiente paso planteado fue analizar cuáles de esas necesidades cubrirá el PGD y cómo este se comportará frente a los otros sistemas y procesos de la entidad.

#### *Procedimiento de respuesta a solicitudes de acceso a la información*

El último capítulo incluido en el documento de capacitación fue el procedimiento para tratar la recepción y respuesta a las solicitudes de acceso a la información, ya que para su correcta comprensión y uso era indispensable abordar las otras temáticas. Con este procedimiento se creó un archivo en MS-Excel con todas las consideraciones que se deben tener en cuenta al momento de atender una solicitud de acceso a la información.

Por otra parte, y en relación con este capítulo, se incluyó un apartado para que los usuarios que estén insatisfechos con la respuesta obtenida –o aquellos a quienes se les haya negado el acceso a la información–, puedan dirigir su inconformidad a una instancia superior, sea para obtener una respuesta a su favor o para que, en definitiva, esos entes superiores aporten una justificación más completa y argumentada de la negativa.

#### *B. Registro Nacional de Bases de Datos (Decreto 886 de 2014)*

La temática abordada en los primeros 8 capítulos del documento “Guía de implementación del decreto 886 de 2014” tiene como objetivo contextualizar al público en general acerca del significado de la ley de protección de datos personales y del Registro Nacional de Bases de Datos, y su importancia para el país como ley estatutaria; el capítulo 9 muestra lo relacionado con el sistema de gestión integral de datos personales; el capítulo 10 presenta un análisis sobre el decreto 886 de 2014; el capítulo 11 trata sobre la Superintendencia de Industria y Comercio como entidad encargada de vigilar el cumplimiento de las normas relacionadas con la administración de datos personales; los capítulos 12 a 15 presentan la forma de implementar el decreto 886 de 2014; el capítulo 16 habla sobre los retos actuales de la protección de datos; y el capítulo 17 se refiere al sistema integral de supervisión inteligente.

Del capítulo 10 en adelante, la temática cambia, aunque se incluyen otros conceptos que permitirán una mejor comprensión de los temas, se cuenta con un grupo de procedimientos e instructivos asociados y relacionados con el Registro Nacional de Bases de Datos y con la ley de protección de datos personales. Es importante que los asistentes tengan una interacción directa con estos procedimientos, para lograr que su aprendizaje se realice al mismo tiempo que reciben la capacitación, es decir, que su aprendizaje se base en los ejemplos entregados.

#### *C. Seguridad de la información (ISO 27001)*

Teniendo en cuenta lo exigido a las entidades públicas en el decreto 2573 de 2014 por el Gobierno colombiano respecto de la seguridad y privacidad de la información y

requests for information access. The next step was to analyze the needs that will be covered by DMP and the behavior about other systems and processes of the entity.

#### *Response procedure to request of information access*

The last chapter included in the training document consisted in the procedure for dealing with receiving and answering to requests for information access, since for the best understanding and using it was essential to address the other issues. Subsequently, a file in MS-Excel was created with all the considerations that must be taken into account when attending a request for access to the information.

On the other hand, it was consider a section so that users who are not satisfied with the reply obtained - or those who have been denied access to the information - can address their non-compliance with a higher instance, in order to obtain a reply in their favor or, ultimately, these higher entities provide an entire justification about the rejection.

#### *B. National Database Registry (Decree 886 of 2014)*

The subject studied in the first eight chapters of the document “Guide to the implementation of Decree 886 of 2014” aims to contextualize the citizens about the meaning of the personal data protection law and the National Database Registry, also its importance for both the country and the statutory law; Chapter 9 describes the themes about the personal data integrated management system; Chapter 10 presents an analysis of Decree 886 of 2014; Chapter 11 deals with the Superintendencia de Industria y Comercio (sectoral authority) as an entity responsible of monitoring compliance with standards about the personal data administration; Chapters 12 to 15 study how to implement Decree 886 of 2014; Chapter 16 discusses the current challenges of data protection; And chapter 17 refers to the intelligent supervision comprehensive system.

Starting from Chapter 10, the subject changes, although other concepts are included which allow a better understanding of the issues. Moreover, a set of procedures and instructions are available about the National Database Registry and the Personal Data Protection Law. It is necessary that the stakeholders have a direct interaction with these procedures, in order that their learning takes place at the same time as they receive the training. In other words, their learning is based on the given examples.

#### *C. Information security (ISO 27001)*

Considering the requirements elaborated to the public entities in Decree 2573 of 2014 by the Colombian Government with respect to the security and privacy of information

and the ISO27001; the research team started an investigation about the Information security including the 2005 and 2013 versions of ISO 27001. Subsequently a documented implementation guide was developed. It allows understanding each implication about managing the information security from the standard and the law perspective. After several revisions, the content of the guide was approved and the topic was classified into more specific contents. So, it can be taught to the attendees in sessions of four hours a week.

It should be remembered that one of the objectives is to train public officials, giving them a basic knowledge, so that they can start a process about the implementation of information security controls by a standard known internationally, such as ISO27001:2013.

### III. Results

One of the researches carried out during the development of this project was aimed at establishing the initial knowledge of the population to which the training was directed. Thus, in order to find the shortcomings of the officials, a survey and an initial stage were applied with situations that can be presented within the framework of the Law on Transparency, decree 886 and ISO 27001 standard. For the survey was counted with the participation of several officials belonging to different public institutions of the city of Pereira, however, and because the courses were given to different groups, these do not present the same number of attendees.

After analyzing the results it was determined that it was necessary to train them in all the topics, this conclusion was reached because of the reasons exposed below.

#### A. Law on transparency

##### *Initial situation*

The difficulties initially encountered are:

- Ignorance of the obligated subjects;
- ignorance of regulatory decrees;
- little clarity about the difference between classified and reserved public information;
- little clarity about the concept of public information;
- little mastery of the components of the burden of proof;
- lack of clarity about information management tools; and
- lack of clarity about the time that a subject has to respond to a request for access to public information.

lo relacionado que se encuentra este tema con la norma ISO27001, el grupo de investigación inició una investigación en el tema de seguridad de la información incluyendo las versiones 2005 y 2013 de la ISO 27001. Posteriormente se desarrolló una guía de implementación documentada que permite comprender todas las implicaciones de gestionar la seguridad de la información desde la perspectiva del estándar y de la ley. Luego de pasar por varias revisiones, se aprobó el contenido de la guía y se desglosó la temática en contenidos más específicos, de manera que estos puedan ser impartidos a los asistentes en sesiones de cuatro horas semanales.

Cabe recordar que uno de los objetivos es capacitar a funcionarios públicos, entregándoles un conocimiento básico, de tal manera que ellos puedan iniciar un proceso de implementación de controles en seguridad de la información usando un estándar conocido a nivel internacional, como lo es la Norma ISO27001:2013.

### III. Resultados

Una de las investigaciones adelantadas durante el desarrollo de este proyecto estuvo dirigida a establecer el grado de conocimiento inicial de la población a la cual iban dirigidas las capacitaciones. Así, con el fin de encontrar las falencias de los funcionarios, se aplicaron una encuesta y un escenario inicial con situaciones que se pueden presentar dentro del marco de la ley de transparencia, el decreto 886 y la norma ISO 27001. Para la encuesta se contó con la participación de varios funcionarios pertenecientes a diferentes instituciones públicas de la ciudad de Pereira, sin embargo, y debido a que los cursos se impartieron a grupos distintos, estos no presentan el mismo número de asistentes. Luego de analizar los resultados se determinó que era necesario capacitarlos en todas las temáticas, a esta conclusión se llegó por las razones que se exponen a continuación.

#### A. Ley de transparencia

##### *Situación inicial*

Las dificultades encontradas inicialmente son:

- desconocimiento de los sujetos obligados;
- desconocimiento de los decretos reglamentarios;
- poca claridad sobre la diferencia entre información pública clasificada y reservada;
- poca claridad sobre el concepto de información pública;
- poco dominio de los componentes de la carga de la prueba;
- poca claridad sobre los instrumentos para la gestión de la información; y
- poca claridad sobre el tiempo que posee un sujeto obligado para responder una solicitud de acceso a la información pública.



*Análisis final*

Al finalizar las capacitaciones (40 Horas), se aplicó un escenario final, similar al usado al inicio del curso, pero esta vez con un mayor grado de dificultad. La temática para la prueba final incluyó:

- la historia de las leyes de acceso a la información;
- la historia de la ley 1712 de 2014;
- los decretos reglamentarios de la ley 1712 de 2014;
- el proceso de caracterización de usuarios;
- los instrumentos para la gestión de la información pública;
- la publicación de datos abiertos; y
- a respuesta a las solicitudes de acceso a la información.

Para este escenario se obtuvo un balance positivo debido a que la mayoría de los funcionarios encontró y justificó las inconformidades, demostrando así dominio del tema, lo que contrasta con la situación previa a la realización de estas capacitaciones, cuando la argumentación del escenario inicial fue casi nula. Las **FIGURAS 1 a 7** se elaboraron con base en la información de los 34 funcionarios que desarrollaron tanto el escenario inicial, como el final, en ellas es posible visualizar que la mejora en el nivel de conocimiento es sustancial y logra superar las dificultades encontradas al comienzo. En todas las figuras, el escenario inicial se registra al lado izquierdo.

*Final analysis*

At the end of the training (40 hours), a final stage was applied, similar to the one used at the beginning of the course, but this time with a greater degree of difficulty. The theme for the final test included:

- History of the laws of access to information;
- history of law 1712 of 2014;
- regulatory decrees of law 1712 of 2014;
- process of characterization of users;
- instruments for the management of public information;
- publication about open data; and
- response to requests for access to information.

For this stage, a positive balance was obtained because most of the officials found and justified the nonconformities, thus demonstrating mastery of the subject, which contrasts with the situation prior to the realization of these trainings, when the argumentation of the initial stage was almost null. **FIGURES 1 to 7** were elaborated based on the information of the 34 officials who developed both the initial and the final stage, in them it is possible to visualize that the improvement

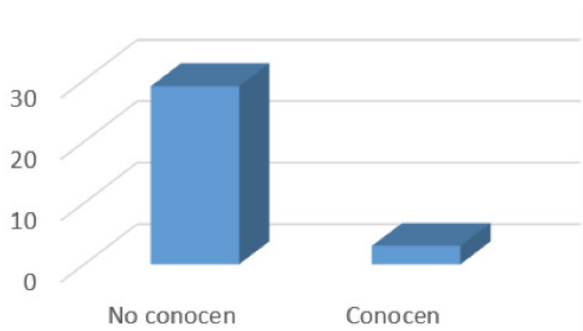


Figure 1. Officials who know the number of obligated subjects / Funcionarios que conocen el número de sujetos obligados

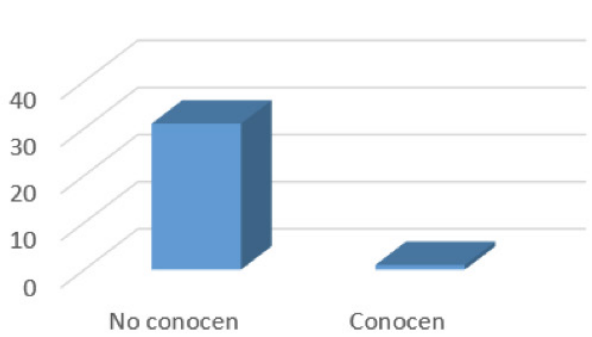
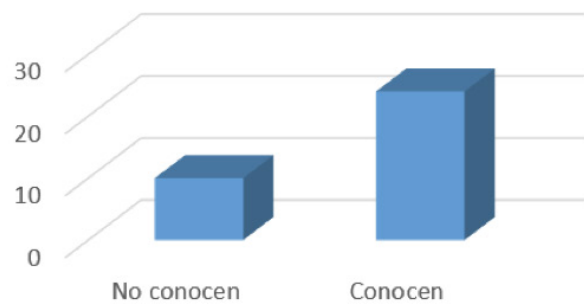


Figure 2. Officials who know the number of regulatory decrees / Funcionarios que conocen el número de decretos reglamentarios

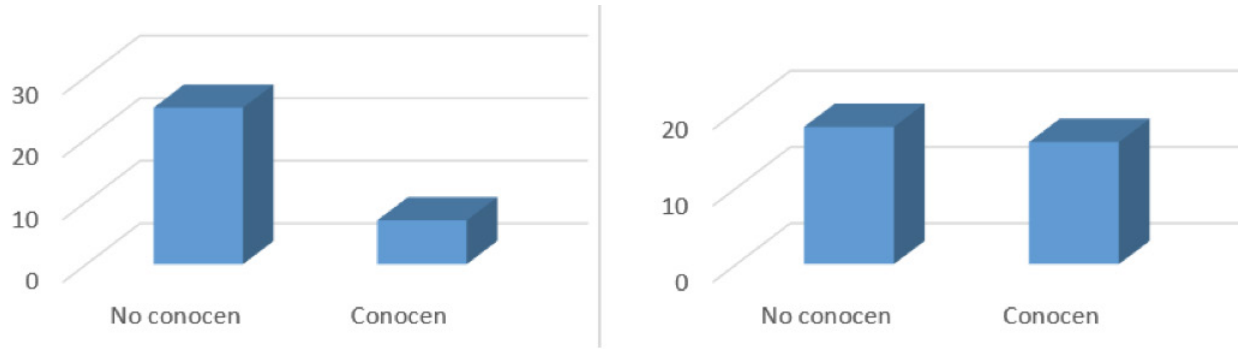


Figure 3. Officials who know the difference between classified and discreet information / Funcionarios que conocen la diferencia entre información clasificada y reservada

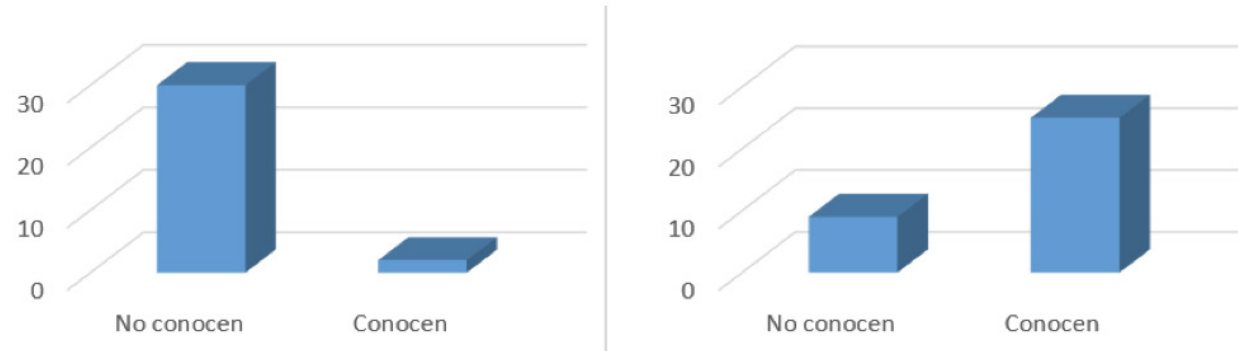


Figure 4. Officials who know the elements that compose the test load / Funcionarios que conocen los elementos que componen la carga de la prueba

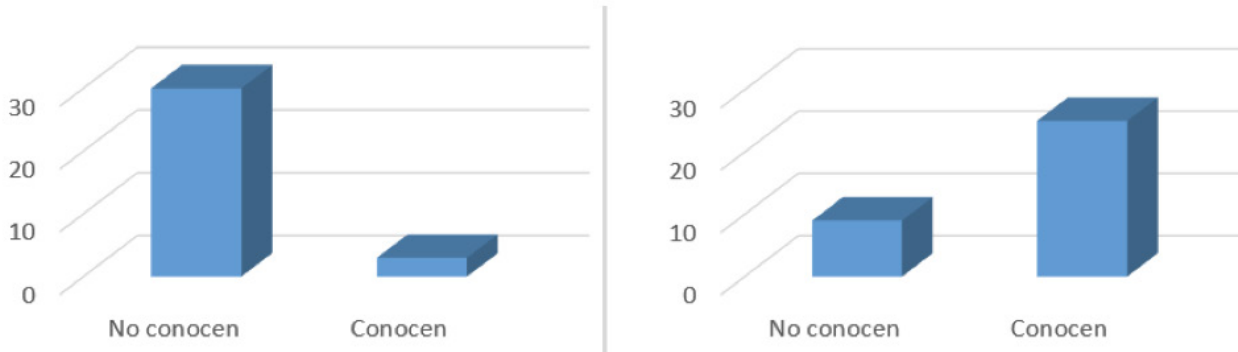


Figure 5. Officials who know the instruments for the information management / Funcionarios que conocen los instrumentos para la gestión de la información

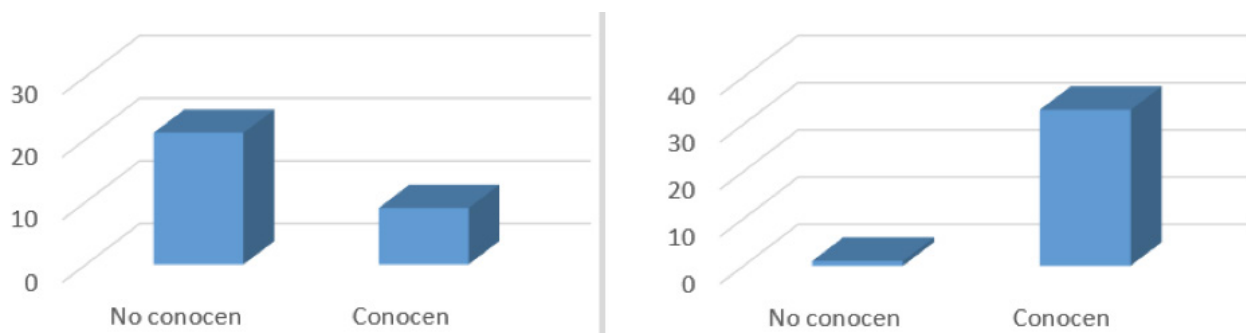


Figure 6. Officials who know the appropriate language to publish the information / Funcionarios que conocen el idioma en que se debe publicar la información

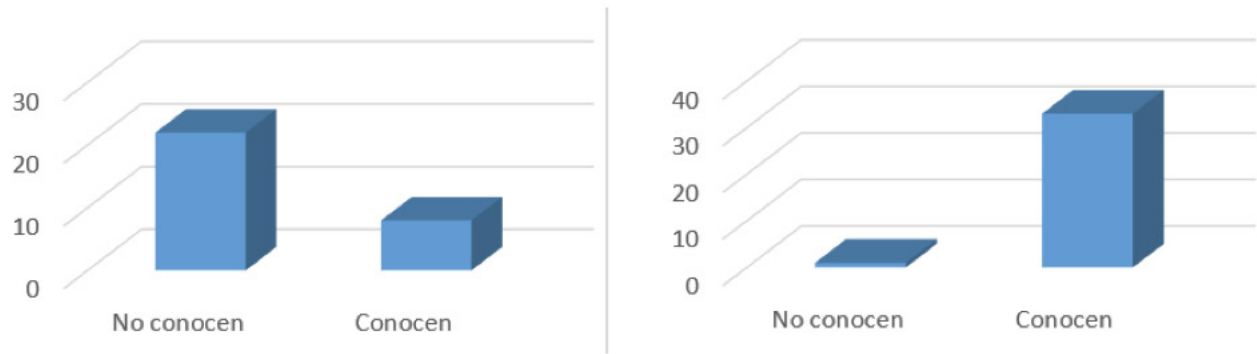


Figure 7. Officials who know the economic cost of access to public information / Funcionarios que conocen el costo económico de acceder a la información pública

### B. Reporte de bases de datos

#### *Situación inicial*

Las dificultades encontradas inicialmente (ver Figura 8) son:

- 52% no tiene claro cuál es la entidad encargada de la administración;
- no es claro si es necesaria la autorización antes de la recolección de los datos;
- algunos funcionarios creen estar obligados a autorizar el tratamiento de datos sensibles;
- 9 de los 23 funcionarios creen que el administrador de la base de datos [DBA] es el mismo responsable y encargado del tratamiento;
- una gran mayoría conoce los plazos para la atención de reclamos; y
- 17,39% afirma que solo se debe registrar las bases de datos digitales, cuando es necesario registrar ambas, físicas y digitales.

#### *Análisis final*

Luego de haber realizado las capacitaciones, en la última sesión se aplicó un escenario final similar al aplicado al comienzo de ellas, aunque con un grado de dificultad y detalle más avanzado. Los resultados de este ejercicio fueron satisfactorios. Como se puede visualizar en la **TABLA 2**, la mejora y nivel de conocimiento es sustancial y logra superar las dificultades encontradas inicialmente.

De este ejercicio es posible concluir que es necesario ahondar un poco más en los temas relacionados con la cesión de datos, las diferencias entre los tipos de datos personales, la delegatura encargada por la SIC para la protección de datos personales, la normativa internacional y los deberes de los encargados.

### C. ISO 27001

#### *Situación inicial*

El escenario inicial permitió conocer, de manera general, qué tanto sabían los funcionarios acerca de los procesos y controles, relacionados con la seguridad de la información, implementados en las entidades donde laboran. En la **TABLA 3** se evidencia que más de la tercera parte de los funcionarios mostró falencias en su conocimiento respecto de la estructura y el detalle de la norma ISO 27001.

in the level of knowledge is substantial and manages to overcome the difficulties found at the beginning. In all figures, the initial stage is recorded on the left side.

### B. Database report

#### *Initial situation*

The difficulties initially encountered (see Figure 8) are:

- 52% are not clear on which entity is in charge of the administration;
- it is not clear whether authorization is necessary prior to data collection;
- some officials believe they are obliged to authorize the processing of sensitive data;
- 9 of the 23 officials believe that the database administrator [DBA] is responsible and in charge of the processing;
- a large majority knows the deadlines for handling complaints; and
- 17.39% affirms that only digital databases should be registered, when it is necessary to register both physical and digital ones.

#### *Final analysis*

After completing the training, in the last session a final stage similar to that applied at the beginning of the training was applied, although with a degree of difficulty and more advanced detail. The results of this exercise were satisfactory. As it can be seen in **TABLA 2**, the improvement and level of knowledge is substantial and overcomes the difficulties encountered initially.

From this exercise it is possible to conclude that it is necessary to deepen a little more in the subjects related to the transfer of data, the differences between the types of personal data, the delegation commissioned by the SIC for the protection of personal data, international regulations and duties of the managers.

### C. ISO 27001

#### Initial situation

The initial stage allowed to know, in a general way, how much the officials knew about the processes and controls, related to information security, implemented in the entities where they work. **TABLE 3** shows that more than a third part of the officials showed shortcomings in their knowledge regarding the structure and detail of the ISO 27001 norm.

#### Final analysis

The last stage established a measurement about the knowledge acquired during the training (**TABLE 4**).

## IV. Final considerations and conclusions

The Law on Transparency represents an anticorruption advance for the country, in so far as it allows the citizens to participate more actively in the issues of interest, nevertheless, in need of a society (citizenship in general and officials) trained and formed to be able to use the tools that the government provides; therefore, it should be emphasized on the population and awareness campaigns should be made known: the law, how to use it and how to report in which entities irregularities or non-compliance occur.

It should be emphasized that the SIC regulations and activities have achieved a pedagogical effect in society. Slowly, Colombians are becoming familiar with a data protection system - different from the classic guardianship mechanism - that seeks to be a guarantor and offer a legitimizing effect of business activities and involves the processing of personal data.

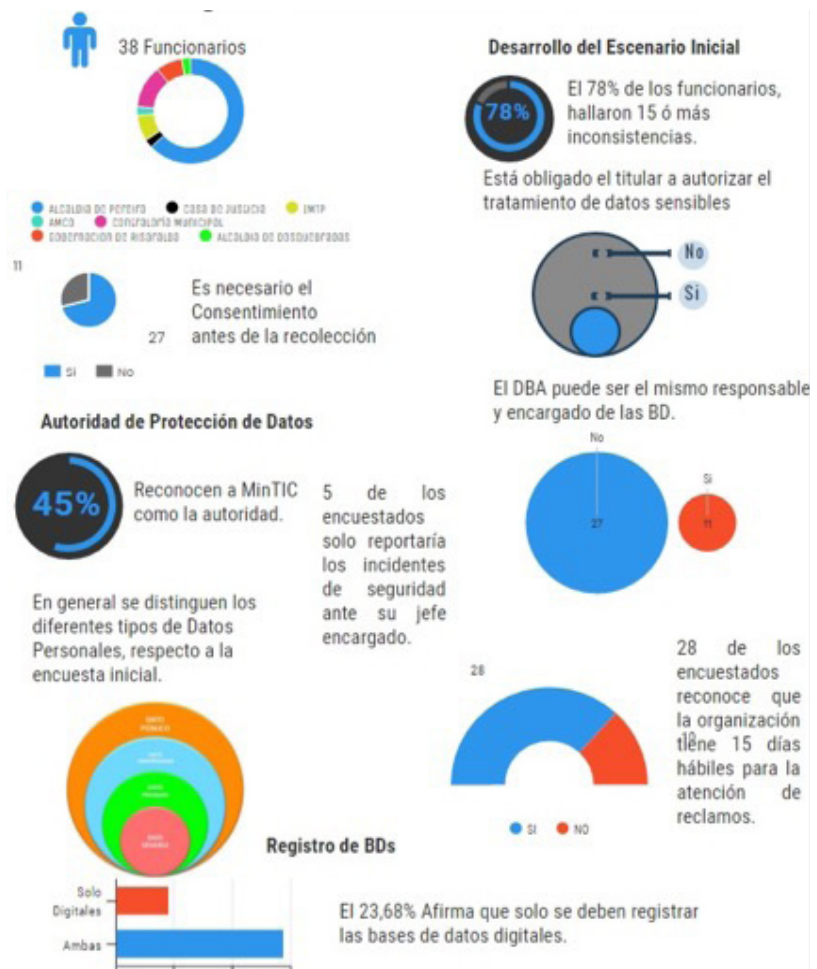
The protection of personal data in children and adolescents is one of the current challenges in this area. For this reason, it is necessary for entities such as the ICBF and the Municipal Education Secretariat to take ownership of the issue, create organizational awareness and ensure protection of the fundamental right to privacy.

#### Análisis final

El escenario final tenía como objetivo medir el conocimiento adquirido durante la capacitación (**TABLA 4**).

## IV. Consideraciones finales y conclusiones

La ley de transparencia representa para el país un avance anticorrupción, en la medida en que permite que la ciudadanía participe más activamente en los temas de interés, no obstante, es necesario contar con una sociedad (ciudadanía en general y funcionarios) capacitada y formada para poder utilizar las herramientas que el gobierno le brinda; por lo tanto, se debe hacer énfasis en la población y realizar campañas de concientización que den a conocer:



#### From the figure:

- Participants: 38 officers
- Found at least 15 inconsistencies (78%)
- DBA must be in charge and responsible (11 from 38)
- Prior authorization is required for data collection (27 from 38)
- MINTIC is the authority for information protection (45%)
- The organization has 15 days to respond to complaints (26 from 38)
- Only digital databases should be registered (23,6%)

Figure 8. Initial stage / Escenario inicial

Table 2. Final stage, answers by theme - law 1581 (n=34 public officers) / Escenario final: respuestas por temática - ley 1581 (n=34 funcionarios públicos)

Law 1581 theme / Temática de la ley 1581	Correct / Correctas	Incorrect / Incorrectas
Delegator / Delegatura	19	15
National normative / Normativa nacional	33	1
International normative / Normativa internacional	30	4
Personals data type / Tipos de datos personales	27	7
Duties of responsible people / Deberes de los responsables	33	1
Giving data / Cesión de datos	22	12
Transfer of data / Transferencia de datos	32	2
Rights ARCARS / Derechos ARCARS	33	1
Payment for service / Cobro por servicio	34	0
Copy of authorization / Copia de la autorización	34	0
Deadline for consultations / Plazos para consultas	33	1
Deadline for complaints / Plazos para reclamos	34	0
Procedibility requirement / Requisito de procedibilidad	32	2
Duties of people in charge / Deberes de encargados	29	5
Channels / Canales	34	0
Treatment policy / Política de tratamiento	34	0
Data transmission / Transmisión de datos	33	1
Deadline for new BDS register / Plazos de registro para nuevos BDS	32	2
Right to oblivion / Derecho al olvido	33	1
<b>MOST RELEVANT / LO MÁS RELEVANTE</b>		
<b>Development of the final stage / Desarrollo de un escenario final</b>		
94% of officials found 18 or more inconsistencies / 94% de los funcionarios halló 18 o más inconsistencias.		
<b>Responsible and people in charge / Responsables y encargado</b>		
More than 90% recognize the differences between responsible and people in charge / Más del 90% reconoce las diferencias entre responsables y encargado.		
<b>Information treatment policy / Política de tratamiento de la información</b>		
The treatment policy should be different for the responsible and each of the caregivers / La política de tratamiento debe ser diferente para el responsable y cada uno de los encargados.		
<b>Derechos de los titulares / Rights of holders</b>		
The rights of holders are clear / Los derechos de los titulares son claros		
<b>Responsible delegator / Delegatura encargada</b>		
Delegator for the protection of personal data / Delegatura para la protección de datos personales.		

la ley, la manera de utilizarla y cómo informar en qué entidades se presentan irregularidades o incumplimientos.

Debe resaltarse como positivo que la normativa y la actividad de la SIC han logrado un efecto pedagógico en la sociedad, lentamente los colombianos se van familiarizando con un sistema de protección de datos –diferente al clásico mecanismo de tutela– que busca ser garantista y ofrecer un efecto legitimador de las actividades empresariales e involucra el tratamiento de datos personales

La protección de datos personales en niños, niñas y adolescentes es uno de los retos actuales en el tema, por esta razón, es necesario que entidades como el ICBF y la Secretaría de Educación Municipal se apropien del tema, creen conciencia organizacional y garanticen la protección de los derechos fundamentales a la privacidad.

Until August 31, 2016, only 5,028 companies out of the 298,318 (the universe: private and mixed economy companies) have been registered, a low figure considering that all of them expire on November 8, 2016.

Information security is the strategic ally to enable business continuity. The implementation, maintenance and continuous improvement of information security systems, through controls and policies, minimize the risks to which entities are exposed in their day-to-day.

Through the survey and the scenario that was applied at the beginning of the training it was possible to establish that the entities in the region do not have personnel with enough domain for the implementation

Table 3. Results of initial stage / Resultados del escenario inicial

65% knows standards—as ISO27001—and concepts about information security.	65,0% conoce de estándares como la norma ISO 27001 y conceptos relacionados con la seguridad de la información.
69,7% Information security policies are known in the labor entity.	69,7 %conoce de las políticas de seguridad de la información en la entidad para la cual labora.
55,9% of entities forgets to provide knowledge to officials about responsibilities on information security.	55,9% de las entidades olvida entregar a los funcionarios conocimiento de las funciones y responsabilidades relacionadas con la seguridad de la información.
More than 33% of officials show low knowledge about structure and details of ISO 27001 standard.	En más de 33% de los funcionarios se evidenciaron falencias en el conocimiento respecto de la estructura y el detalle de la norma ISO 27001.

Table 4. Results of the final stage / Resultados del escenario final

Total of Resolved Scenarios: 42/ Total escenarios resueltos: 42	
Initial Scenario: 15 questions/ Escenario inicial: 15 preguntas	
Final Scenario: 30 questions/ Escenario final: 30 preguntas	
Initial stage lets an overview about the officers level of knowledge about their organization information security procedures and controls (result: 80%) / El escenario inicial permitió dar a conocer, de manera general, qué tanto sabían los funcionarios acerca de los procesos y controles implementados en la entidad donde laboran, respecto de la seguridad de la información (resultado 80%).	
Final stage objective was measure knowledge acquired during the training process, then, the officer responses should be accurate and specific (result: 66,7%) / El escenario final tenía como objetivo medir el conocimiento adquirido durante la capacitación; el funcionario debía dar respuestas más específicas y exactas (resultado 66,7%).	

of law 1712, decree 886 and ISO 27001; therefore, it is essential to carry out the training on this subject, for the benefit not only of the entity, but also of the citizenship. The course developed delivered satisfactory results, therefore, it can be replicated in several institutions of the region and the country.

Through the survey and the scenario employed at the beginning of the training, it was concluded that none of the entities in the region had adequate appropriation of law 1712 of 2014, decree 886 and ISO 27001, for its implementation; However, after the training process, it was evidenced that there was appropriation of the knowledge transmitted. Currently, these officials constitute an institution reference in order to implement each of the knowledge.

This positive impact will be reflected, both the entities and their employees. Through the knowledge acquired, they will help to improve the users perception regarding the processes carried out in the organization, as well as the institutional offer improvement and the functions performance, working hand in hand with the civil population and other users interested in strengthening institutional management, to fulfill the duties that have a level Legislative and / or Normative.

Hasta el 31 de agosto de 2016 se han registrado solo 5.028 empresas de las 298.318 que conforman el universo (privadas y de economía mixta), una cifra baja si se considera que a todas ellas se les vence el plazo el 8 de Noviembre de 2016.

La seguridad de la información es el aliado estratégico para permitir la continuidad del negocio. La implementación, el mantenimiento y la mejora continua de los sistemas de seguridad de la información, a través de los controles y las políticas, minimiza los riesgos a los que las entidades se encuentran expuestas en su día a día.

A través de la encuesta y el escenario que se aplicó al comienzo de las capacitaciones se pudo establecer que las entidades en la región no poseen personal con el dominio suficiente para la implementación de la ley 1712, el decreto 886 y la ISO 27001; por consiguiente, es indispensable realizar las capacitaciones en esa temática, para beneficio, no solo la entidad, sino también de la ciudadanía. El curso desarrollado arrojó resultados satisfactorios, por consiguiente, se puede replicar en varias instituciones de la región y el país.

A través de la encuesta y el escenario aplicados al comienzo de las capacitaciones se pudo establecer que las entidades en la región no poseían la suficiente apropiación de la ley 1712 de 2014, el decreto 886 y la ISO 27001, para su implementación; sin embargo, luego del proceso de formación realizado se pudo evidenciar que hubo apropiación de los conocimientos transmitidos y ahora estos funcionarios son un referente en la institución para la implementación y puesta en marcha de cada uno de ellos.

Este impacto positivo se verá reflejado, tanto en las entidades, como en sus funcionarios, ya que a través del conocimiento adquirido, estos ayudarán a mejorar la percepción de los usuarios con respecto a los procesos que se realizan actualmente en la organización, así como el mejoramiento de su oferta institucional y del desempeño de las funciones realizadas, trabajando de la mano con la población civil y los demás usuarios e interesados en el fortalecimiento de la gestión institucional, para dar cumplimiento a los deberes que se tengan a nivel legislativo y/o normativo.

Por ello, la creación de los procedimientos, plantillas e instructivos entregados y desarrollados durante el tiempo que duraron las capacitaciones son elementos valiosos para las entidades públicas, ya que estos permiten mejorar sus procesos y la atención al usuario, creando así una cadena de confianza de la ciudadanía hacia las entidades, y de las entidades hacia sus funcionarios, lo que permite que estos últimos puedan aspirar, a través de sus competencias y buenas prácticas institucionales, a un mejor nivel salarial o a un mejor cargo en la institución. *S&T*

Therefore, the creation of procedures, templates and instructions developed along the training are valuable elements for public entities, due to they allow to improve the processes and the user service. Hence a chain of Trust Citizenship towards entities is created. Thus, the officials can obtain a better salary level or a better position in the institution, through their skills and good institutional practices. *S&T*

## Referencias / Referencias

- Decreto 2573 de 2014. (2014, diciembre 12). *Diario Oficial No. 49363*. Bogotá, Colombia: Imprenta Nacional.
- Decreto 886 de 2014. (2014, mayo 13). *Diario Oficial No. 49150*. Bogotá, Colombia: Imprenta Nacional.
- Delgado, M. (2009). Formación Profesional: la problematización como estrategia didáctica para la intervención profesional pedagógica [paper in "II Coloquio de Investigación educativa UIM FES Acatlán, México]. Available at: [http://www.academia.edu/1206743/La\\_problematización\\_como\\_estrategia\\_didáctica\\_para\\_la\\_intervención](http://www.academia.edu/1206743/La_problematización_como_estrategia_didáctica_para_la_intervención)
- Departamento Nacional de Planeación [DNP]. (2014). *Guía de caracterización de ciudadanos, usuarios y grupos de interés*. Bogotá, Colombia: DNP. Available at: <https://colaboracion.dnp.gov.co/CDT/Programa%20Nacional%20del%20Servicio%20al%20Ciudadano/Guia%20de%20Caracterizaci%C3%B3n%20de%20Ciudadanos.pdf>
- Departamento Nacional de Planeación [DNP]. (2009). *Guía Metodológica para la Formulación de Indicadores*. Bogotá, Colombia: DNP. Available at: <https://www.dnp.gov.co/LinkClick.aspx?fileticket=-hBkmozjehk%3D&tabid=1214>
- Instituto Colombiano de Normas Técnicas [ICONTEC] (2013). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Norma Técnica Colombiana NTC-ISO-IEC 27001*. Bogotá, Colombia: ICONTEC.
- Ley 1712 de 2014. (2014, marzo 6). *Diario Oficial No. 49084*. Bogotá, Colombia: Imprenta Nacional.
- Ley 1341 de 2009. (2009, julio 30). *Diario Oficial No. 47.426*. Bogotá, Colombia: Imprenta Nacional.
- Más información más derechos [Web site]. (2014). Retrieved from: <http://masinformacionmasderechos.co/>
- Ministerio de las Tecnologías de la Información y las Comunicaciones. (2011). *Guía para la caracterización de usuarios de las entidades públicas*. Bogotá, Colombia: MinTIC. Available at: [http://estrategia.gobiernoonline.gov.co/623/articulos-8536\\_recurso\\_1.pdf](http://estrategia.gobiernoonline.gov.co/623/articulos-8536_recurso_1.pdf)
- Newman, V. (2015). *Datos personales en información pública: oscuridad en lo privado y luz en lo público*. Bogotá, Colombia: Dejusticia. Available at: [http://www.dejusticia.org/files/r2\\_actividades\\_recursos/fi\\_name\\_recurso.699.pdf](http://www.dejusticia.org/files/r2_actividades_recursos/fi_name_recurso.699.pdf)
- Organización de los Estados Americanos [OEA]. (2010). *Ley modelo interamericana sobre acceso a la información pública* [CP/CAJP-2840/10]. Available at: [https://www.oas.org/dil/esp/CP-CAJP-2840-10\\_Corr1\\_esp.pdf](https://www.oas.org/dil/esp/CP-CAJP-2840-10_Corr1_esp.pdf)

## CURRICULUM VITAE

**Edward Fabián Penagos Granada** Computational Systems Engineer from Universidad Tecnológica de Pereira [UTP], Colombia (2014), currently he is pursuing his last semester of the Master in Systems and Computing –emphasis in networks and telecommunications– at the UTP, where also he is a researcher / Se graduó como Ingeniero de Sistemas de Computación en la Universidad Tecnológica de Pereira [UTP], Colombia en 2014. Actualmente se encuentra realizando el último semestre de la Maestría en Ingeniería de Sistemas y Computación con especialidad en Redes Telecomunicaciones en la UTP, donde además trabaja como investigador.

**Ana María López Echeverry** Electrics Engineer from Universidad Tecnológica de Pereira [UTP], Colombia (1996). At the Universidad Pontificia Bolivariana, Medellín, Colombia, she obtained two degrees: Specialist in Telecommunications (2012) and Master in Engineering (2013). She has thirteen years of experience as professor at the UTP, also she has been evaluator pair in calls about cyber-security, health, tourism, etc. Currently she is a professor at the UTP (Systems and Computing Engineering) and research about: information security, cryptography and advanced communication protocols / Se graduó en Ingeniería Eléctrica en la Universidad Tecnológica de Pereira [UTP], Colombia, en 1996; En la Universidad Pontificia Bolivariana [UPB] de Medellín, Colombia obtuvo sus grados como Especialista en Telecomunicaciones (2012) y Máster en Ingeniería (2013). Cuenta con trece años de experiencia docente universitaria en la UTP. Se ha desempeñado como par evaluadora de convocatorias en el área de TI en temas de ciberseguridad, salud y turismo, entre otras. Actualmente se desempeña como docente en el Programa de Ingeniería de Sistemas y Computación y como investigadora en las áreas de seguridad de la información, criptografía y protocolos de comunicación avanzados, en la UTP.

**Paula Andrea Villa Sánchez** She obtained her degrees as: Computational Systems Engineer (2001), Specialist in Data Networks (2007) and Master in Computing and Systems Engineering –emphasis in Security of Information and Software Quality– (2014) at the Universidad Tecnológica de Pereira [UTP], institution where also she has worked as teacher and researcher / Se graduó en la Universidad Tecnológica de Pereira [UTP], Colombia, como: Ingeniera de Sistemas de Computación (2001); Especialista en Redes de Datos (2007); y Magister en Ingeniería de Sistemas y Computación con especialidad en Seguridad de la Información y Calidad de Software (2014). Ha trabajado como docente e investigadora en la UTP.