IMPLEMENTACIÓN DE POLÍTICA DE PROTECCIÓN DE DATOS PARA LA FUNDACIÓN ESCUELA CONTRA LA POBREZA - CONSULTORIA EMPRESARIAL

CHRISTIAN LEONARDO GONZÁLEZ HINCAPIÉ

UNIVERSIDAD AUTÓNOMA DE MANIZALES

FACULTAD DE ESTUDIOS SOCIALES Y EMPRESARIALES

MAESTRÍA EN ADMINISTRACIÓN DE NEGOCIOS

MANIZALES

2024

IMPLEMENTACIÓN DE POLÍTICA DE PROTECCIÓN DE DATOS PARA LA FUNDACIÓN ESCUELA CONTRA LA POBREZA - CONSULTORIA EMPRESARIAL

Autor

CHRISTIAN LEONARDO GONZÁLEZ HINCAPIÉ

Proyecto de grado para optar al título de Magister en Administración de Negocios

Directora

PAULA ZULUAGA ARANGO

Co Directora

LINA VICTORIA BERRÍO RÍOS

UNIVERSIDAD AUTÓNOMA DE MANIZALES

FACULTAD DE ESTUDIOS SOCIALES Y EMPRESARIALES

MAESTRÍA EN ADMINISTRACIÓN DE NEGOCIOS

MANIZALES

2024

RESUMEN

Este proyecto de consultoría se centra en el diseño e implementación de una política de protección de datos para la Fundación Escuela Contra la Pobreza, una organización sin fines de lucro en Manizales, Colombia, que maneja información sensible de beneficiarios, donantes y colaboradores. Dados los crecientes riesgos en el manejo de datos personales y la importancia de los derechos de habeas data, un diagnóstico organizacional reveló la necesidad de mejorar las prácticas en la recolección, almacenamiento y protección de datos.

A través del análisis de riesgos, un marco estratégico y el desarrollo de procedimientos y controles específicos, se estableció una política de protección de datos. Esta política no solo cumple con la normativa colombiana, sino que también respalda la misión y la visión de la fundación. Los resultados indican que la política mejorará la seguridad y la confianza de los datos, optimizando la toma de decisiones y la gestión de los mismos.

Palabras claves: Protección de datos, habeas data, seguridad

ABSTRACT

This consulting project focuses on the design and implementation of a data protection policy for Fundación Escuela Contra la Pobreza, a non-profit organization in Manizales, Colombia, that handles sensitive information of beneficiaries, donors and collaborators. Given the increasing risks in the handling of personal data and the importance of habeas data rights, an organizational diagnosis revealed the need to improve practices in data collection, storage and protection.

Through risk analysis, a strategic framework and the development of specific procedures and controls, a data protection policy was established. This policy not only complies with Colombian regulations, but also supports the mission and vision of the foundation. The results indicate that the policy will improve data security and trust, optimizing decision making and data management.

Key words: Data protection, habeas data, security.

CONTENIDO

1 INTRODUCCIÓN 10

2 SITUACIÓN ACTUAL DE LA ORGANIZACIÓN 11

2.1 CONTEXTO HISTÓRICO DE LA ORGANIZACIÓN 11

2.2 PROBLEMÁTICA IDENTIFICADA 12

2.3 DIAGNÓSTICO DE LA ORGANIZACIÓN 13

3 JUSTIFICACIÓN 18

4 REFERENTE TEÓRICO 23

4.1 HABEAS DATA 23

4.2 SEGURIDAD DE LA INFORMACIÓN 26

4.3 POLÍTICA DE GESTIÓN DE LA INFORMACIÓN 30

4.4 LA TOMA DE DECISIONES EN LA ORGANIZACIÓN Y LA GESTIÓN DE DATOS 32

5 OBJETIVOS 35

5.1 OBJETIVO GENERAL 35

5.2 OBJETIVOS ESPECÍFICOS 35

6 METODOLOGÍA DE LA CONSULTORÍA 36

7 DESARROLLO DE LA CONSULTORÍA 38

7.1 DIAGNÓSTICO 38

7.2 CONSTRUCCIÓN DE LA POLÍTICA 41

7.2.1 Elementos de la Planeación Estratégica 41

7.2.2 Política de protección de datos 43

7.3 PROCEDIMIENTOS Y CONTROLES PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE PROTECCIÓN DE DATOS 43

7.3.1 Construcción de Elementos del Direccionamiento Estratégico 43

7.3.2 Estructuración de Matriz de Riesgos 45

7.3.3 Elaboración del Mapa de Procesos 46

7.3.4 Construcción del Indicador 47

7.3.5 Capacitación y Formación 49

8 CONCLUSIONES 50

9 REFERENCIAS BIBLIOGRÁFICAS 54

10 ANEXOS 59

LISTA DE TABLAS

Tabla 1 Amenazas desde la Dimensión de Seguridad 14

Tabla 2 Escala de Valores para el Cálculo de la Probabilidad. 15

Tabla 3 Escala de Valores para el Cálculo del Impacto. 16

Tabla 4 Ejemplos de Posibles Daños 16

Tabla 5 Ejemplo de Preguntas para Identificar Amenazas. 22

Tabla 6 Fases de la Consultoría. 36

Tabla 7 Matriz del Riesgo 40

Tabla 8 Plataforma estratégica desarrollada 43

Tabla 9 Matriz de Riesgo Aceptable 45

Tabla 10 Parámetros de Construcción del Indicador 1, Organización de Seguridad de la Información 47

Tabla 11 Parámetros de Construcción del Indicador 2, Cubrimiento del SGSI en Activos de Información 48

TABLA DE FIGURAS

Figura 1Escala de Valores 17

Figura 2Análisis PESTEL. 42

Figura 3 Mapa de Procesos Fundación Escuela Contra la Pobreza..... 46

TABLA DE FOTOGRAFÍAS

Foto 1 Capacitación Habeas Data Voluntarios..... 49

Foto 2 Capacitación política de tratamiento de datos lideres de la fundación 49

LISTA DE ANEXOS

Anexo 1 Encuestas Realizada a Lideres de la Fundación Escuela Contra la Pobreza 59

Anexo 2 Política de Protección de Datos Personales Fundación Escuela Contra la Pobreza 59

Anexo 3 Guía de Indicadores de Gestión Para la Seguridad de la Información Ministerio de las TIC´S. 59

Anexo 4 Disclaimer Entrada a Eventos de la Fundación. 59

Anexo 5 Disclaimer Asistencia 59

Anexo 6 Disclaimer Autorización Datos Personales Menor de Edad 59

Anexo 7 Disclaimer Autorización Persona Jurídica 59

Anexo 8 Mapa de Procesos 59

Anexo 9 Acta de Realización Matriz PESTEL y POAM 59

1 INTRODUCCIÓN

En el presente trabajo de consultoría, se profundizará en el estudio del *habeas data* desde las políticas de gestión de datos e información desde un componente organizacional. El *habeas data* es un derecho fundamental que garantiza a las personas el control y protección de sus datos personales, así como el acceso a la información que se encuentra en las bases de datos de las entidades públicas y privadas.

La necesidad de proteger todos los datos relativos a las personas no es algo accidental, pues estos datos representan el registro de su vida, reflejan sus características, sus opciones importantes y sus debilidades. El tratamiento adecuado de los datos personales es una exigencia de la dignidad de la persona y del libre desarrollo de la personalidad. El conocimiento por parte de otros de una información que una persona no ha querido revelar afecta seriamente a la forma en que esta se desenvuelve normalmente en la sociedad, la manera en que es vista por sus familias, por sus vecinos, o sus compañeros de trabajo (Ordóñez, 2019).

Para el caso de esta consultoría, en la Fundación Escuela Contra la Pobreza este derecho es especialmente relevante ya que se manejan datos personales de donantes, beneficiarios, empleados y voluntarios.

La información personal está disponible en múltiples plataformas y sistemas, es de fundamental importancia que esté gestionada y protegida, por lo que nadie debería inmiscuirse en ella, si no es con su autorización, garantizando el derecho a la privacidad e intimidad. El objetivo de esta consultoría se basará en la implementación del *habeas data* desde la gestión de datos e información para garantizar políticas y procedimientos claros para la recopilación, el uso, la divulgación y la eliminación de datos personales que además de dar cuenta de las obligaciones legales y éticas que se ejecutan en sus actividades de gestión social como fundación, serán un insumo significativo en la gestión estratégica de la fundación contando con la trazabilidad de la información que brinde seguridad y confianza a cada uno de los stakeholders

2 SITUACIÓN ACTUAL DE LA ORGANIZACIÓN

2.1 CONTEXTO HISTÓRICO DE LA ORGANIZACIÓN

La Fundación Escuela Contra la Pobreza es una organización sin fines de lucro fundada en 2006 por líderes comunitarios de la comuna San José, una zona vulnerable de la ciudad de Manizales. La organización establece y administra espacios educativos alternativos con el objetivo de formar individuos productivos que sean responsables con la sociedad y que contribuyan progresivamente a su desarrollo personal y social. Esto se promueve a través de procesos alternativos de inclusión e integración en la sociedad, de manera que garanticen el desarrollo humano y contribuyan a la superación de la pobreza, desarrollando un aporte significativo al Objetivo de Desarrollo Sostenible (ODS) 1 fin de la pobreza, (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO])

Desde su inicio, la *Fundación Escuela Contra la Pobreza* se ha concentrado en el trabajo con los grupos que presentan mayor nivel de vulnerabilidad de la ciudad, especialmente niños, niñas y adolescentes. Desde allí, la fundación ha tenido un impacto positivo en la vida de más de 6.000 niños cada año a través de la implementación de talleres de integración, realización de actividades recreacionales y deportivas, clases de formación para la vida, donación de alimentos, entre otras iniciativas que buscan contribuir al mejoramiento de la realidad social de estos grupos poblacionales.

Es importante destacar que la Fundación Escuela Contra la Pobreza actúa como un eje articulador, entre la empresa privada y las organizaciones públicas, de manera que todos los interesados involucrados en el desarrollo de cada una de las iniciativas creadas, reconozcan la importancia de contribuir a la sociedad desde acciones explícitas que garanticen un goce pleno a los derechos desde la igualdad y equidad.

2.2 PROBLEMÁTICA IDENTIFICADA

La *Fundación Escuela Contra la Pobreza,* ha llevado a cabo varios proyectos que desde su inicio han generado un impacto positivo en la vida de los niños, niñas y adolescentes de la comuna San José. Estos proyectos que incluyen espacios de educación alternativa para la vida buscan con el trabajo colaborativo de diversos actores, mejorar la calidad de vida de estos grupos poblacionales considerados los más vulnerables de la ciudad de Manizales.

El principal propósito de esta iniciativa es brindar a la Fundación la asistencia necesaria que direccione la calidad en la consolidación de la información obtenida en el desarrollo de sus actividades y le sea de utilidad en los procesos administrativos y gerenciales. Con este proceso de consultoría, se espera que la fundación establezca los esquemas adecuados para formalizar y adoptar buenas prácticas de protección de datos personales, garantizando la seguridad de la información sensible de la población y respetando el derecho a la intimidad de cada persona que ha hecho parte de las actividades planteadas.

Pese a que la Fundación lleva varios años desarrollando sus actividades con procesos inclusivos y de integración social logrando impactar cada vez más sectores vulnerables, no cuenta con el desarrollo e implementación de una política de tratamiento de datos personales, tal como lo determina la Ley Estatutaria 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”, según lo dispuesto el 17 de octubre de 2012. D.O. No. 48587 (Congreso de la República, 2012). Se identifica entonces, la necesidad latente de mejorar las estrategias de recopilación y almacenamiento de datos personales, que le permita cumplir con los procesos legales y éticos de la organización, además de convertirse en un insumo significativo para la gestión estratégica permitiendo el cumplimiento de sus metas a corto y largo plazo y contando con una trazabilidad de la información que brinde seguridad y confianza a cada uno de los stakeholders.

De igual manera, se identifica que la fundación carece de una adecuada plataforma estratégica, en donde si bien tiene claro su objetivo de impactar desde un acompañamiento integral a la población vulnerable de Manizales, no cuenta con el desarrollo formal de plataforma estratégica que incluye aspectos como misión, visión y valores agregados, que le permitan cumplir con sus objetivos a largo plazo y establecer un direccionamiento que marque las rutas de logro y alcance, que les brinde posibilidades para identificar dónde se encuentra y hacia dónde se dirige. Asimismo, no cuentan con un proceso de documentación, almacenamiento y adecuado manejo de la información y datos personales obtenidos de las personas que han sido impactadas en el desarrollo de sus actividades, como causa de la falta de implementación de una política de protección de datos apropiada que facilite su gestión y garantice las buenas prácticas y seguridad de la información.

2.3 DIAGNÓSTICO DE LA ORGANIZACIÓN

Dentro del desarrollo de la consultoría a la Fundación, se evidencia la creación de los estatutos, la existencia del acta de constitución de su mesa directiva y los registros del desarrollo de reuniones periódicas realizadas para la planeación de las actividades. Sin embargo, no se identifican elementos que permitan revelar ejercicios de evaluación, planeación estratégica y análisis de oportunidades de mejora tales como la identificación de sus fortalezas, debilidades, oportunidades y amenazas, que puedan afectar el logro de los objetivos estratégicos establecidos como organización y a su vez, les permitan proyectar las posibilidades de crecimiento

De la misma manera, se evidencia que, a pesar de estar legalmente constituida, carece de algunos procesos administrativos y organizacionales que pueden influir en el desempeño de sus actividades. Uno de los más importantes, se centra en el área financiera, en donde si bien la Fundación se financia por medio de las donaciones recibidas de los actores involucrados para el desarrollo de las actividades que permiten la inclusión y la integración social dirigidas al grupo poblacional identificado con características de vulnerabilidad, no cuenta con herramientas e indicadores eficaces que permitan el manejo y control de la información que sustente el que hacer de la organización, tales como cantidad

de beneficiarios por grupo, valor invertido por individuo, impacto total alcanzado, entre otros .

Igualmente, no se evidencia la adecuada administración y gestión de la información de los datos de beneficiarios, donantes, directivos y voluntarios que participan en cada una de las actividades realizadas por la Fundación, elemento fundamental que debe de ser gestionado de manera estratégica para la construcción de indicadores significativos para sus stakeholders, además del cumplimiento del marco legal que permita prevenir riesgos como organización sin ánimo de lucro, que trabaja en pro de la primera infancia, niñez y adolescencia en estado de vulnerabilidad.

En este sentido, y con el fin de identificar y evaluar las probabilidades e impactos derivados las situaciones identificadas, se realiza el análisis de riesgos, el cual tiene como objetivo establecer acciones que prevengan, reduzcan o eviten en lo posible, la posibilidad de ocurrencia y que permita minimizar la exposición a los riesgos, y establecerlo en un nivel aceptable.

Cabe resaltar que, desde la perspectiva de la normatividad de protección de datos personales, existen tres amenazas desde la dimensión de seguridad: confidencialidad, integridad y disponibilidad, como se presentan en la Tabla 1. Estas amenazas pueden afectar la vida y la intimidad de las personas, por lo que es necesario prever los factores que puedan tener un impacto negativo en su vulneración (Agencia Española Protección de Datos, 2021).

Tabla 1 Amenazas desde la Dimensión de Seguridad

Acceso ilegitimo de datos	*Confidencialidad*
Modificación no autorizada de los datos	*Integridad*
Eliminación de los datos	*Disponibilidad*

Fuente: Agencia Española de Protección de Datos (2021)

De acuerdo a lo analizado, se identifica que para poder prevenir estas amenazas se debe entender el ciclo de vida de los datos, identificando los posibles escenarios que puedan producir una violación de estos o de la libertad del sujeto. Teniendo en cuenta las tres dimensiones del daño más importantes que se podrían presentar en las actividades de la Fundación, se identifica que las posibles aristas son:

- Daño físico: acciones que pueden ocasionar un daño en la integridad física del interesado.
- Daño material: acciones que pueden ocasionar pérdidas económicas, patrimoniales, laborales, etc.
- Daño moral: acciones que pueden ocasionar un daño moral o mental en el interesado, como una depresión, fobias, acoso, etc.

La evaluación de riesgos consiste en estimar la probabilidad y el impacto de que la amenaza se materialice. Por tanto, el riesgo se asume como aquel proceso intrínseco que se le presenta a cada actividad donde se requiere el tratamiento de datos. En relación con los parámetros mencionados, las escalas de valores para calcular la probabilidad de ocurrencia del riesgo y el impacto de este se describen en las Tabla 2 y 3, respectivamente, y fueron tomadas de la Agencia Española de protección de datos. Cabe anotar que en estas no se tienen en cuenta las medidas que mitigan el riesgo. (AEPD, 2021)

Tabla 2 Escala de Valores para el Cálculo de la Probabilidad.

PROBABILIDAD	DESCRIPCIÓN	VALORACIÓN
Probabilidad despreciable	Posibilidad de ocurrencia muy baja, sucede de forma fortuita	Se valorará con 1
Probabilidad limitada	Posibilidad de ocurrencia baja, sucede de forma ocasional	Se valorará con 2
Probabilidad significativa	Posibilidad de ocurrencia alta, sucede con bastante frecuencia	Se valorará con 3
Probabilidad máxima	Posibilidad de ocurrencia muy elevada, sucede con mucha frecuencia	Se valorará con 4

Fuente: Agencia Española Protección de Datos (2021).

Tabla 3 Escala de Valores para el Cálculo del Impacto.

IMPACTO	DESCRIPCIÓN	VALORACIÓN
Impacto despreciable	Impacto muy bajo, sus consecuencias son prácticamente despreciables sin impacto sobre el interesado	Se valorará con 1
Impacto limitado	Impacto bajo, sus consecuencias suponen un daño menor sin impacto sobre el interesado	Se valorará con 2
Impacto significativo	Impacto alto, sus consecuencias suponen un daño elevado con impacto sobre el interesado	Se valorará con 3
Impacto máximo	Impacto muy alto, sus consecuencias suponen un daño muy elevado con un impacto crítico sobre el interesado	Se valorará con 4

Fuente: Agencia Española Protección de Datos (2021).

De esta manera, la Tabla 4 proporciona ejemplos del impacto de posibles riesgos que puedan ocurrir.

Tabla 4 Ejemplos de Posibles Daños

Tipo de Impacto	Ejemplo de Daño
Despreciable: los interesados no se veran afectados o encontraran alguna pequeña inconveniencia	- Molestia o irritación. - Se incumplen las obligaciones materiales sin perjuicio relevante.
Limitado: los interesados podrán encontrar incovenientes no significativos	- Estrés o padecimientos fisicos menores. - Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos. - Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
Significativo: los interesados encontrarán consecuencias significativas, que deberían poder superar sin dificualtades	- Empoderamiento del estado de salud o agreciones. - Se agrede contra los derechos y libertades de los interesados, por ejemplo: una citación judicial, entrar en una lista de morosidad o divulgación de información con impacto significativo en la reputación del interesado.

Máximo: los interesados encontrarán consecuencias significativas o incluso irreversibles, que podrían no llegar a superarse.	- Se agrede significativamente contra los derechos y libertades de los interesados, padecimientos psicológicos con consecuencias a largo plzo o irreparables por la divulgación de datos sensibles.

Fuente: Agencia Española de Protección de Datos (2021).

Así entonces, se precisa que la escala de valores con la cual será determinado el impacto para el caso de la fundación es aquella que tiene un valor mínimo de uno (1) o despreciable, hasta un máximo de cuatro (4), valor por el cual se multiplicará cada amenaza para identificar el dato de impacto y obtener así el respectivo resultado de la matriz de riesgo, tal como se presenta en la Figura 3.

Figura 1Escala de Valores

Probabilidad	Máxima 4	4	8	12	16
	Significativa 3	3	6	9	12
	Limitada2	2	4	6	8
	Despreciable 1	1	2	3	4
Bajo	Alto	Despreciable* 1	Limitada *2	Significativa *3	Máxima *4
Medio	Muy Alto				

Fuente: Agencia Española de Protección de Datos (2021)

3 JUSTIFICACIÓN

La Constitución Política Colombia determina que somos un Estado Social de Derecho, por lo que dentro de sus objetivos y finalidades está la de garantizar la efectividad de los “derechos y deberes consagrados en la Constitución”. Asimismo, apunta que las “autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades” (Constitución Política de Colombia, 1991, Artículo 2).

Además, el Artículo 6 superior indica que, “Los particulares sólo son responsables ante las autoridades por infringir la Constitución y las leyes. Los servidores públicos lo son por la misma causa y por omisión o extralimitación en el ejercicio de sus funciones” siendo enfático en que los servidores públicos deben ejercer sus funciones con una observancia integra a la norma constitucional y a los reglamentos (Constitución Política de Colombia, 1991, Artículo 6).

Para la división tripartita del poder público, estos son los mayores recolectores, beneficiarios y circuladores de datos personales, que en algunas ocasiones son responsables o encargados de su tratamiento, ya sea porque acuden a terceros (como los contratistas, aplicaciones, empresas de tecnología y seguridad de la información o entre entidades públicas) que asumen el trabajo del tratamiento de datos. Sin embargo, no implica que la empresa principal pierda la responsabilidad de garantizar el adecuado uso de la información.

En consonancia con el Artículo 15 constitucional, las personas tienen el derecho a conocer, actualizar y rectificar toda la información que se haya recogido sobre ellas en las bases de datos o archivos de entidades públicas y privadas. De igual forma, señala que en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (Constitución Política de Colombia, 1991, Artículo 15).

Este mandato constitucional fue desarrollado por la Ley Estatutaria 1581 de 2012, la cual aplica a las entidades privadas y entidades estatales. En este sentido la norma de *habeas data* define "Tratamiento" como "cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión" (Congreso de la República, 2012, Artículo 3, literal g). Debido a que, las entidades públicas tratan millones de datos de personas y que deben obrar conforme a la Constitución y a la ley, deben garantizar dentro de sus instituciones la aplicación de la Ley Estatutaria 1581 de 2012 y sus decretos (Congreso de la República, 2012).

Desde otro ángulo, se destaca la importancia de los datos como aspecto clave para el desarrollo y evaluación dentro de su modelo de gestión. La etapa de seguimiento y trazabilidad, permite a las organizaciones conocer su desempeño actual en el medio, al mismo tiempo que muestra perspectivas y decisiones futuras, con la posibilidad de analizar en tiempo real. El objetivo de contar con indicadores es apoyar la gestión organizacional, sin importar el sector, para que sea eficiente y eficaz al facilitar la evaluación permanente de la gestión y el mejoramiento continuo de la organización (Beltrán J, 2005)

La Fundación Escuela Contra la Pobreza, como participante del tercer sector, está obligada por la Ley Estatutaria 1581 de 2012 a aplicar y desarrollar la protección de datos personales, debido a el flujo de información que maneja de terceras personas en el desarrollo de sus actividades misionales. A pesar de ello, no cuenta con una política interna que permita garantizar al titular de la información personal, el derecho a conocer, actualizar y rectificar toda la información que se haya recogido sobre ellos en sus bases de datos o archivos de la organización. Lo anterior imposibilita el análisis y monitoreo de los datos personales en cuanto a su disponibilidad, integralidad y confidencialidad, para prevenir riesgos económicos y sociales, tanto de los titulares como de la entidad. Desde este panorama, el objetivo de la consultoría para la Fundación consiste en la implementación de una política de protección de datos personales para garantizar la seguridad de la información y el derecho a la seguridad de la información desde el goce pleno a la privacidad al mismo tiempo que, serán los datos un insumo significativo en la gestión

estratégica contando con la trazabilidad de la información para brindar seguridad y confianza a cada uno de los stakeholders.

El derecho a la privacidad se define como la libertad, la facultad que toda persona tiene de desenvolverse en el ámbito social, familiar o personal, de acuerdo a sus propios patrones de conducta, hábitos o costumbres. El derecho a decidir en qué medida compartirá con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal, comprende los aspectos muy particulares de la identidad individual, la voz, la imagen, la edad, la nacionalidad, la salud, los hábitos sexuales, las ideas religiosas, políticas, filosóficas, la situación patrimonial, financiera; en suma, sus datos estrictamente personales. Por otro lado, la imparable revolución de las TIC ha dado lugar a que este derecho se regule jurídicamente a fin de proteger la libertad y la intimidad, amenazados por el acopio de datos y la existencia de sofisticados sistemas de registros automatizados en entidades públicas y privadas (Quiroz, 2016).

La recopilación y organización de los datos, es un proceso primordial para que una empresa o institución pueda desarrollar sus actividades y relaciones con sus clientes y proveedores. A partir de esa enorme cantidad de datos en constante crecimiento, las empresas que son capaces de extraer información relevante toman sus decisiones, por lo cual requieren de una base de datos que contengan datos fundamentales de las personas, con el manejo seguro y confiable de las mismas. Al referir la seguridad de las bases de datos se deben considerar los niveles de seguridad: seguridad física (control de acceso físico), seguridad de sistemas operativos (*Hardening*), seguridad a nivel de red (software de red), seguridad a nivel humano (métodos de acceso) y seguridad a nivel de gestión de base de datos (privilegios de usuarios base de datos) (Machuca, 2022). Es fundamental que la Fundación Escuela Contra la Pobreza integre desde sus políticas internas una recopilación de datos basada en la seguridad y el buen uso de la información personal, ya que en su mayoría son datos de menores de edad que se encentran en constante situación de vulnerabilidad.

Los cambios sociales y tecnológicos llevaron a establecer sobre este derecho varias denominaciones que pretenden desarrollar no solamente su fundamento sino también el instituto de garantía que comprende. Puede decirse que la modernidad no solo ha significado el más radical y antes impensable salto tecnológico y científico logrado por los humanos, sino la consolidación de valores nuevos, y el derrumbe de otros. Desde esta perspectiva, el acceso a las tecnologías es una de las características y prioridades de la sociedad moderna. No obstante, se han desvalorizado los riesgos que supone la sobreexposición de la persona y de su información personal. Siendo así, el derecho a la protección de datos se fundamenta en que quien trata datos personales, trata información ajena, no propia, que debe utilizar con estricto respeto a los derechos del interesado. Esta construcción nos reconduce al respeto a la dignidad de la persona (Ordoñez, 2019).

En cualquier caso, no se protegen los datos en sí mismos, sino a los titulares de esos datos. El objeto de resguardo es la autodeterminación informativa, que consiste en la libertad de un titular respecto de cómo disponer de sus datos personales, cualquiera sea la naturaleza de estos, es decir, no solo aquellos referidos al ámbito de su intimidad o privacidad, sino incluso los aparentemente inocuos, con miras a desarrollar un proceso de autoconstrucción de su personalidad en sociedad, y replicar las consecuencias indeseadas de valoraciones no deseadas, no autorizadas, equivocadas o inexactas. La Fundación Escuela Contra la Pobreza de manera relevante, debe realizar la implementación de una política que garantice la protección a los datos personales, ya que ésta es también un eje articulador de garantía de otros derechos fundamentales (Ordoñez, 2019).

De acuerdo con lo anterior, se presenta en la tabla 5 algunos ejemplos de preguntas de utilidad para la identificación de las posibles amenazas que puede presentar cualquier tipo de organización. La aplicación de estas preguntas hacia la organización ha sido de utilidad para el desarrollo de la consultoría al interior de la fundación escuela contra la pobreza.

Tabla 5 Ejemplo de Preguntas para Identificar Amenazas.

Tipo de Amenaza	Amenaza	¿Qué preguntas pueden formular para identificar las amenazas?
Acceso ilegitimo a los datos	• Pérdidas de dispositivos móviles. • Fuga de información. • Acceso intencionado por parte de personal no autorizado. • Ataques intencionados (*hacking*, suplantación de identidad, etc.). • Uso ilegitimo de datos personales.	• ¿Los dispositivos electrónicos están cifrados?
Eliminación de datos	• Error humano o ataque intensivo que provoca borrado pérdida de datos. • Desastres naturales.	• ¿Los datos pueden ser eliminados únicamente por el personal autorizado?

Fuente: agencia española de protección de datos

4 REFERENTE TEÓRICO

4.1 HABEAS DATA

El recurso de agravio constitucional denominado *Habeas Data*, es una garantía que protege dos derechos fundamentales: el derecho a la información y la autodeterminación informativa o protección de datos personales. Ambos, forman parte del ámbito de los derechos humanos, reconocidos y protegidos por los Tratados Internacionales y las Cartas Constitucionales de los diferentes países en los que impera el estado de derecho (Quiroz, 2016).

Para comprender la importancia de la protección de datos en las organizaciones debemos entender cuáles son los tipos de datos personales, donde los podemos encontrar y que protegen; como también los sujetos que intervienen en el proceso del manejo de la información, para que así la entidad pueda asumir la responsabilidad que tiene en su rol de manejo adecuado de la información.

Los tipos de datos personales se clasifican en:

Datos Públicos: es aquel dato que no sea semiprivado, privado o sensible. Estos datos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. Por ejemplo: datos generales de identificación de la persona, datos de ubicación relacionados con actividad comercial (dirección, correo y teléfono empresarial), datos relacionados con el estado civil de las personas, su profesión u oficio, etc. (Presidencia de la República, 2013).

Dato Semiprivado: es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector personas o a la sociedad en general, como el dato financiero y crediticio. Por ejemplo: datos financieros, datos patrimoniales, datos de actividad económica, declaración de renta, etc. (Superintendencia de Industria y Comercio, 2022).

Datos Privados: es el que por su naturaleza íntima o reservada sólo es relevante para el titular, por ejemplo: datos de ubicación personal, socioeconómicos, tributarios, datos de historia laboral, nivel educativo, gustos e intereses particulares, fotografías y videos, antecedentes, documentación comercial, números telefónicos, direcciones correo electrónico personal, etc. (Congreso de la República, 2008).

Datos Sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. Por ejemplo: datos biométricos de la persona, descripción morfológica, relacionados con la salud, relacionados con el estado de salud, pertenencia a sindicatos, organizaciones sociales, creencias religiosas, políticas, preferencia referencia, orientación sexual, origen étnico, población en condición vulnerable, datos personales de niños, niñas o adolescentes sin autorización de sus padres o representantes legales (Congreso de la República, 2012, Artículo 5).

A continuación, se presenta la definición de algunos términos utilizados regularmente:

Titular: persona natural cuyos datos personales sean objeto de tratamiento (Congreso de la República, 2012, Artículo 3, literal f).

Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Congreso de la República, 2012, Artículo 3, literal g).

Encargado del Tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del Tratamiento (Superintendencia de Industria y Comercio, 2016).

Fuente o Responsable del Tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos (Superintendencia de Industria y Comercio, 2016).

Según la Constitución Política Colombiana en su Artículo 15 expresa que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley (Constitución Política de Colombia, 1991, Artículo 15).

A partir de 2011, se comienza a entender gracias a la Corte Constitucional, el *habeas data* como un derecho autónomo y los mecanismos que garanticen su aplicación no dependen solo de los jueces, sino de la institución administrativa facultada o designada para ejercer eficiente control y vigilancia a los sujetos de derecho público y privado encargados del manejo de datos personales1. La Ley Estatutaria 1581 de 2012 entrega la competencia a la Superintendencia de Industria y Comercio –SIC, la cual cuenta con un organismo interno denominado Delegatura para la protección de datos personales, la cual deben velar por el

efectivo cumplimiento de las normativas legales sobre este tema (Corte Constitucional de Colombia, 2011).

El ser humano ha tenido un avance vertiginoso en el mundo de la tecnología, donde cada vez surgen nuevos sistemas que recolectan información de las personas, generando dudas sobre si el uso de esta información personal es el apropiado, debido a que muchas veces es de carácter sensible, lo que plantea una necesidad de brindar una adecuada protección a la información que se recolecta y a la que circula en la web. Tal como lo plantea
Bedoya (2014), "En la vida cotidiana los ciudadanos entregan sus datos personales en innumerables situaciones y a distintas entidades, lo cual los hace vulnerables frente a usos ilegítimos de la información. Basta con dar una ojeada a la historia para encontrar situaciones específicas en donde los datos de las personas han sido utilizados para fines poco ortodoxos, entre otros los de señalamiento y discriminación masiva que han traído terribles consecuencias para la humanidad".

Esto plantea una discusión sobre la privacidad de las personas y sus libertades como individuos, no solo en el territorio colombiano, si no, más allá, en un mundo digital globalizado, "No obstante, estas visiones —y regulaciones— tienen claros limitantes territoriales que no permiten una protección global a un fenómeno global. La autorregulación aparece como una herramienta capaz de ampliar la protección de los individuos más allá de las fronteras" (Ornelas e Higuera, 2013).

4.2 SEGURIDAD DE LA INFORMACIÓN

La necesidad de proteger todos los datos relativos a las personas no es algo anecdótico, pues ellos representan el registro de su vida, reflejan sus características, sus opciones vitales, sus debilidades. El tratamiento adecuado de los datos es una exigencia de la dignidad humana y del libre desarrollo de la personalidad. El conocimiento por parte de otros de una información que una persona no ha querido revelar, afecta seriamente a la forma en que esta se desenvuelve normalmente en la sociedad, la manera en que es vista

por sus familias, por sus vecinos o por sus compañeros de trabajo. Los avances tecnológicos han permitido su difusión masiva, situación que pone en riesgo a las personas y aumenta exponencialmente los daños a sus derechos fundamentales (Naranjo-Godoy, 2017).

La necesidad de los controles de los datos personales en Colombia surgió debido a que la informática trajo consigo una nueva forma de poder intangible sobre los derechos de las personas, su intimidad, vida e información personal; otorgando una protección muy limitada a estos derechos por parte de las normas existentes. Para proteger a las personas de la capacidad de acumular datos que proporcionaba la tecnología a unos sujetos, datos que individualmente no podrían causar daño a la persona, pero acumulados, podrían simbolizar un perjuicio para las personas, se necesitaba restablecer un equilibrio entre los que entregan los datos con quienes los manejan (Duran, 2015).

El derecho a la protección de datos personales tiene su origen en la intimidad, del que se separa gradualmente hasta que se reconoce su autonomía a través de la jurisprudencia y posteriormente de la incorporación de normativa constitucional, legal e incluso reglamentaria. Inicialmente, por su antecedente inmediato se atendía únicamente datos considerados íntimos, o aquellos que tenían un nivel adicional de protección, los denominados datos sensibles, que "permitan identificar a la persona, confeccionando su perfil ideológico, racial, sexual, económico, o de cualquier otra índole (Naranjo-Godoy, 2017).

El marco legal de la protección de datos personales en Colombia es una mixtura del Artículo 15 de la Constitución Política de Colombia de 1991 con más de setenta normas promulgadas desde 1951. Salvo la Ley 1266 de 2008, todas las demás disposiciones hacen referencia marginal a pocos temas sobre la materia. Se trata de regulaciones sectoriales que referencialmente mencionan ciertos aspectos en torno a determinados datos personales (Remolina-Angarita, 2010).

Muy pocas normas aluden al *habeas data* y hacen referencia a los datos personales en general. La mayoría de ellas trata sobre información personal especial, como los datos de identificación dactilar, las historias clínicas, los datos obtenidos en censos de población; los datos relacionados con la seguridad social; el dato comercial y financiero, los antecedentes penales, los datos de género; los datos de las niñas, niños y adolescentes e información sobre personas con discapacidades (Remolina-Angarita, 2010).

El derecho a la privacidad se define como la libertad, la facultad que toda persona tiene de desenvolverse en el ámbito social, familiar o personal, de acuerdo a sus propios patrones de conducta, hábitos o costumbres. Por lo que nadie debe inmiscuirse en ella, si no es con su autorización. El derecho a decidir en qué medida compartirá con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal, comprende los aspectos muy particulares de la identidad individual, la voz, la imagen, la edad, la nacionalidad, la salud, los hábitos sexuales, las ideas religiosas, políticas, filosóficas, la situación patrimonial, financiera; en suma, sus datos estrictamente personales. Por otro lado, la imparable revolución de las TIC ha dado lugar a que este derecho se regule jurídicamente a fin de proteger la libertad y la intimidad, amenazados por el acopio de datos y la existencia de sofisticados sistemas de registros automatizados que se encuentran en entidades públicas y privadas (Quiroz, 2016).

En cualquier caso, no se protegen los datos en sí mismos, sino a los titulares de esos datos. El objeto de resguardo es la autodeterminación informativa, que consiste en la libertad de un titular respecto de cómo disponer de sus datos personales, cualquiera sea la naturaleza de estos, es decir, no solo aquellos referidos al ámbito de su intimidad o privacidad, sino incluso los aparentemente inocuos, con miras a desarrollar un proceso de autoconstrucción de su personalidad en sociedad, y replicar las consecuencias indeseadas de valoraciones no deseadas, no autorizadas, equivocadas o inexactas (Naranjo-Godoy, 2017).

Es el derecho que tiene toda persona de acceder y controlar la información personal registrada en bancos de datos públicos o privados, es el único que ejerce las facultades de:

a) Solicitar la corrección, rectificación, actualización o modificación de datos inexactos. b) Solicitar la cancelación de datos obsoletos, inapropiados o irrelevantes. c) Facultad de solicitar la cancelación de datos personales obtenidos por procedimientos ilegales. c) Facultad de exigir que se adopten medidas suficientes para evitar la transmisión de datos a personas o entidades no autorizadas. Como tal, faculta a los individuos a decidir qué datos son los que pueden o no ser conocidos, autorización que debe ser expresa, porque es ella quien controla la información o los datos que se refieren a su persona, que no es más que la forma de preservar su privacidad, frente al peligro de las bases de datos y al uso de las nuevas tecnologías y sus potentes herramientas de acopio y procesamiento, que ha generado nuevas modalidades de amenaza y agresión a los derechos y libertades, tipificados como delitos informáticos (Quiroz, 2016).

En consecuencia, debe atribuirse mayores niveles y garantías de protección a los datos personales, "es conveniente insistir en que la protección de datos personales es también un instituto de garantía de otros derechos fundamentales", ya que la influencia y repercusión de la recopilación, tratamiento y difusión de los datos personales afectan directamente el ejercicio de las libertades individuales en una sociedad en la que lo virtual y lo real se interrelacionan constantemente (Naranjo-Godoy, 2017).

De otro modo, Laudon y Laudon (2016) y Miguel (2015), indican que un mal manejo y control de la seguridad en las organizaciones puede generar pérdidas económicas por las acciones legales que pueden emprender en contra de ellos los entes de control; de ahí la importancia de la implementación de mecanismos y estrategias por parte de las empresas para proteger su información y la de sus clientes.

Por todo lo anterior, se considera que se debe recurrir a la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), se debe adoptar el modelo de procesos "Planificar - Hacer-Verificar-Actuar (PHVA), según lo estipula la Norma ISO/IEC 27001 (ISO, 2013).

4.3 POLÍTICA DE GESTIÓN DE LA INFORMACIÓN

Todos los ciudadanos tenemos derecho a conocer, actualizar y rectificar toda la información que se almacene o se recopile en las bases de datos administradas por empresas privadas o entidades públicas. Este derecho está contemplado en la Ley Estatutaria 1581 de 2012, conocida como el Régimen General de Protección de Datos Personales, en el que, además, se señalan los principios y obligaciones que tienen todos aquellos que realicen el tratamiento de datos personales para garantizar la protección del derecho fundamental de *habeas data* (Superintendencia de Industria y Comercio, 2012).

Los responsables y encargados del tratamiento de datos personales tienen la obligación de tener un manual interno de políticas y procedimientos en el que se expliquen claramente todos los parámetros y reglas que utilizará la organización para garantizar el correcto tratamiento de los datos personales, en especial, el procedimiento que la organización utilizará para atender las quejas, consultas y reclamos presentados por los titulares en ejercicio de su derecho de *habeas data*. Para ello, la organización o responsable de los datos podrá utilizar documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular (Superintendencia de Industria y Comercio, 2012).

Las políticas de tratamiento de la información deben contener, como mínimo, lo siguiente:

- Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable del tratamiento de los datos.
- Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando no se haya informado mediante aviso de privacidad.
- Derechos que tiene el titular de la información.
- Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y/o revocar la autorización.

- Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
- Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

Las entidades públicas y privadas están cada vez más expuestas a sufrir incidentes de seguridad digital, lo cual, puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Razón por la cual se deben de diseñar, adoptar y promover políticas, planes, programas y proyectos en el uso y apropiación de las TIC, estableciendo lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones (Ministerio de Tecnologías de la Información y las Comunicaciones, 2021).

La política de gestión de la información se establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las entidades públicas y privadas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la entidad enmarcados en su modelo de operación por procesos (Ministerio de Tecnologías de la Información y las Comunicaciones, 2021).

La información es uno de los activos más importantes de una organización para el buen desempeño de sus labores y el éxito en el campo en que trabaja. El desarrollo de una gestión estratégica, basada en información oportuna, de calidad y pertinente para la toma de decisiones, garantiza la disminución de los riesgos asociados a la misma. La Política de Gestión de Datos e Información Institucional, establece los lineamientos basados en una estrategia que responda a los retos institucionales y permita el buen gobierno de los datos y

la información, de cara a la necesidad de fortalecer la toma de decisiones, la rendición de cuentas y las necesidades diarias para el buen funcionamiento (Universidad del Rosario, 2021).

Esta política parte del reconocimiento de los datos institucionales como un activo estratégico; esto es, la consideración de que los datos son la base fundamental para extraer información acerca de la comunidad, el entorno, las acciones, tendencias y efectividad de las apuestas realizadas, entre muchas otras opciones. De manera general, se ve a los datos institucionales como herramienta que ayuda a la innovación y el logro de los objetivos estratégicos que se han propuesto. Este reconocimiento, tal como toda distinción de un activo y su valor, implica la necesidad del diseño de un sistema de manejo, gobierno y uso de este activo, a fin de garantizar que su utilización sea adecuada, ética y responsable, velando por la calidad, objetividad, legalidad, preservación y actualización de los datos (Universidad del Rosario, 2021).

4.4 LA TOMA DE DECISIONES EN LA ORGANIZACIÓN Y LA GESTIÓN DE DATOS

La toma de decisiones se constituye en un proceso esencial en todos los contextos organizacionales, orientado a minimizar riesgos, resolver problemas y aprovechar oportunidades. Por lo tanto, desarrollar procesos de decisión efectivos no solo genera una ventaja competitiva y mejora el posicionamiento en el entorno de negocios, sino que también crea capacidades organizacionales que permiten adaptarse y orientarse mejor a los cambios.

La gestión organizacional y la toma de decisiones y basadas en datos, se apoya en hechos, indicadores e información que guía las decisiones estratégicas alineadas con las con las metas, los objetivos y alcances de una organización. El volumen de datos que se obtienen actualmente es muy elevado, por ello al realizarlo de una manera organizada y controlada puede convertirse en una herramienta efectiva para la organización. El cuidado

de la información y su almacenamiento, genera una cultura al interior de la organización creando procesos y herramientas definidas basadas en la información disponible.

De acuerdo a Citroen (2011, p 494) una organización usa información estratégicamente para percibir los cambios de su ambiente, crear nuevo conocimiento para innovar y tomar decisiones acerca de sus cursos de acción. En este sentido, puede considerarse que los datos son un elemento fundamental que afectan las decisiones estratégicas y el desempeño organizacional como resultado de la participación de los stakeholders dentro y fuera de la organización (Jansen et al., 2011, p.734). Las decisiones estratégicas, son una tarea esencial para la dirección, debido a que permite a las organizaciones alinear sus recursos y capacidades con las amenazas y oportunidades que existen en el medio ambiente.

En la literatura, se identifican diferentes autores como Hubert (1980), Moody (1983), Choo (1998, 2003), Pinto y Gakvez (1999), han abordado la relación entre la gestión de la información, el conocimiento y la toma de decisiones. Esta se evidencia en los enfoques teórico-conceptuales de los procesos gerenciales. Sin embargo, el enlace conceptual no es suficiente para explicar este vínculo y se hace necesario profundizar en las prácticas y dinámicas organizacionales que pueden influir en su construcción.

La gestión de la información puede definirse como “el proceso mediante el cual se obtienen y utilizan los recursos (económicos, físicos, humanos y materiales) básicos para manejar información hacia adentro y para la sociedad a la que sirve” (Ponjuán, 2004). Por su parte, Best (2010), la describe como la coordinación económica, eficiente y efectiva de la producción, control, almacenamiento, recuperación y diseminación de información de recursos externos e internos, con el fin de mejorar el desempeño de la organización. Po tanto, la gestión de la información y su proyección hacia la toma de decisiones organizacionales implica el diseño de una estructura informacional basada en una Política y una Estrategia de Información. Estas deben resaltar la necesidad de disponer de información relevante en todos los niveles de decisión organizacional: estratégico, táctico y operativo.

Como parte de este enfoque, es esencial diseñar una infraestructura conformada por Sistemas de Información que respondan a cada uno de estos niveles, proporcionando recursos y fuentes de información para la búsqueda, procesamiento, análisis y uso de la información necesaria para la toma de decisiones. Para asegurar el desarrollo del proceso más que la disponibilidad, custodia y almacenamiento de la información, y que se convierta en herramienta para la toma de decisiones se identifican los siguientes pasos para su ejecución:

- Identificación de necesidades de información relevante para la toma de decisiones.
- Diseño de flujos de información específicos para cada nivel de decisión.
- Desarrollo de procesos informacionales que intervienen en la toma de decisiones.
- Implementación de gestión documental.
- Implementación de la política de datos y cumplimiento del Habeas Data.

El desarrollo de estos mejoraría la disponibilidad de información, y el conocimiento necesario para tomar decisiones. Estos procesos contribuirían a la creación de productos y servicios de información destinados a la toma de decisiones, cuyos usuarios serían los stakeholders de la organización.

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Establecer los procesos organizacionales necesarios para la implementación de una política de protección de datos en la Fundación Escuela Contra la Pobreza, que permita fortalecer la seguridad, confidencialidad y privacidad de la información.

5.2 OBJETIVOS ESPECÍFICOS

1. Realizar un diagnóstico de la situación actual de la Fundación con respecto a la planeación estratégica y la protección de datos, donde se identifiquen las fortalezas, debilidades y riesgos existentes.
2. Construir un documento con la política de protección de datos de la Fundación que cumpla con las regulaciones de privacidad y se adapte a las necesidades de la organización.
3. Establecer los procedimientos y controles mínimos necesarios que intervienen en la implementación de la política de protección de datos, que cumplan la reglamentación y apoyen los procesos de toma de decisiones organizacionales

6 METODOLOGÍA DE LA CONSULTORÍA

Para esta consultoría se realizó un diagnóstico del estado actual de la Fundación para identificar sus fortalezas, debilidades, oportunidades y amenazas, esto incluirá revisiones de documentos internos, entrevistas con el personal y miembros de la fundación, y análisis de datos relevantes. Posteriormente se definirán los objetivos en colaboración con la fundación para que estos sean claros, medibles y que sean relevantes para la construcción de su plataforma estratégica que incluya la misión y visión. Se realizará una revisión de la normativa vigente con respecto a las políticas de protección de datos en Colombia que sustenten la implementación de esta en la organización. También, desde la planeación se desarrollará un plan estratégico que establezca las acciones necesarias para alcanzar los objetivos establecidos identificando áreas claves de enfoque, la asignación de recursos, el establecimiento de indicadores de rendimiento y la definición de responsabilidades al igual que la identificación de riesgos de la organización frente al manejo de datos personales. Finalmente se plantea un proceso de monitoreo, evaluación de la política de protección de datos implementada en la organización para garantizar la sostenibilidad de misma en todos los procesos realizados en sus actividades, así como la consideración del manejo de datos para la toma de decisiones organizacionales.

La consultoría será desarrollada bajo la siguiente estructura de trabajo en tres fases, las cuales se describen en la Tabla 6:

Tabla 6 Fases de la Consultoría.

Fase	Actividad	Registro
Diagnóstico situacional	Reunión inicial con titular de la Fundación para la fijación de los objetivos.	• Definición de los objetivos de la consultoría.
	Análisis situacional de la Fundación para identificar las fortalezas, debilidades, y riesgos de la misma.	• Revisión de documentos. • Aplicación de instrumento de recolección de datos. • Documento diagnóstico.

Construcción de política	Revisión y análisis de normativa y regulación aplicada a la seguridad de la información de la organización. Redacción del documento final de política de protección de datos.	• Documento final de la política.
Procedimientos y controles para la implementación de la política de protección de datos	Construcción de direccionamiento estratégico. Misión, visión propósito y valores.	• Documento con direccionamiento estratégico.
	Estructuración de matriz de riesgos.	• Documento con matriz de riesgos.
	Elaboración del mapa de procesos.	• Documento de mapa de procesos.
	Construcción de mínimo un indicador estratégico que evidencie la medición y seguimiento de la política de protección de datos.	• Indicador.

Fuente: construcción propia

7 DESARROLLO DE LA CONSULTORÍA

7.1 DIAGNÓSTICO

Para poder realizar el acompañamiento a la Fundación, se realizó un análisis de la situación del funcionamiento y procesos administrativos que esta lleva a cabo. Se logra evidenciar que actualmente la Fundación Escuela contra la Pobreza se encuentra legalmente constituida con la implementación de los estatutos que orientan las acciones que buscan desarrollar. Igualmente, se identifica la conformación de su mesa directiva, así como la definición clara de su población objeto a intervenir, las actividades que se van a desarrollar para el reconocimiento e integración social. Por último, se logra identificar los escenarios de ejecución de las actividades y todos los bienes económicos con lo que cuenta como organización.

En este sentido, se identifica que la Fundación carece de una planeación estratégica que garantice la seguridad de toda la información manejada en sus actividades presentando la posibilidad de enfrentarse a varios desafíos y limitaciones sociales, legales y económicas como organización. Es importante señalar que no se observa una dirección clara frente al adecuado manejo de la información y de los datos personales de las personas impactadas, en este caso se estima que son más de 5.000 mil niños involucrados en las actividades que ha realizado la fundación desde su creación. Sin embargo, no se evidencia cual ha sido la forma de administrar y registrar esos datos personales, el correcto almacenamiento ni el uso de indicadores con evidencias tangibles.

La situación anterior, puede llevar a la dificultad en la identificación del enfoque y la toma de decisiones que no necesariamente están alineadas con los objetivos generales y estratégicos de la organización y, por tanto, como resultado una falta de relación y coordinación entre los diferentes departamentos y equipos que conforman actualmente la organización llevando a dificultades como la duplicación de esfuerzos, conflictos internos y externos e incluso problemas legales por no garantizar como entidad perteneciente al tercer sector, un adecuado manejo de los datos personales incluidos.

Sin una adecuada planeación estratégica del manejo de los datos, la organización puede verse obligada a reaccionar constantemente a los cambios y desafíos del entorno llevándola a decisiones apresuradas. Esta falta de previsión representa la dificultad en la capacidad de la organización para adaptarse y aprovechar oportunidades de crecimiento y desarrollo, de tal manera que también presenta inconvenientes para el fomento de la innovación dentro de la organización. Sin una estrategia clara, la organización puede quedarse rezagada en un mercado competitivo y perder oportunidades de mejora y expansión, con referencia al manejo de los recursos de los donantes involucrados en las actividades de integración social.

En ese mismo sentido, la organización no presenta claridad en las estrategias para el establecimiento de indicadores claves de desempeño y la implementación de mecanismos de seguimiento y evaluación, tanto para el impacto de las actividades como para la administración y uso de los datos personales garantizando la seguridad de la información. Sin estos componentes, la organización puede presentar dificultades para ejecutar mecanismos de medición sobre su progreso, o realizar los ajustes necesarios a tiempo, en su enfoque estratégico.

Así entonces, la carencia de una planeación estratégica frente al manejo de la información, fundamentalmente, de los datos personales de los beneficiarias, donantes, directivos y voluntarios que participan en las actividades, se limita la capacidad de la Fundación para establecer un direccionamiento claro frente a sus objetivos, relacionamiento con sus stakeholders y su organización administrativa interna, de manera que le permita adaptarse a los cambios que trae la sociedad en la nueva era de la tecnología. Desde allí, se hace necesario diseñar e implementar una política de protección de datos que permita desde una planeación estratégica novedosa, alcanzar los objetivos propuestos previniendo los posibles riesgos internos y externos de la organización.

Con el fin de identificar y evaluar la probabilidad e impacto negativos derivados de que una amenaza se potencialice, el análisis de riesgos tiene como objetivo establecer las acciones que prevengan, reduzcan o eviten en la medida de lo posible el surgimiento de

esas amenazas y que permita minimizar a un nivel aceptable la exposición a los riesgos. En este caso, identificaremos los riesgos de la fundación para concretar acciones que mitiguen o eliminen dicho riesgo.

Para ese trabajo, se clasificará el riesgo en los siguientes niveles según lo identificado en las falencias de la Fundación Escuela Contra La Pobreza, como se muestra en la Tabla 7.

Tabla 7. Matriz del Riesgo

Tipo de amenaza	Amenaza	Riesgo	Probabilidad	Impacto	Riesgo inherente
Acceso ilegítimo a los datos	Fuga de información	Terceras personas acceden a los datos vulnerado su confidencialidad	Significativa Valoración: 3	Significativo Valoración: 3	**Alto Valoración: 9**
	Operaciones de tratamiento no autorizadas	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Máxima Valoración: 4	Limitado Valoración: 2	**Alto Valoración: 8**
Modificación no autorizada de los datos	Ataque de software malicioso (Ciberataque)	Se modifican o suplantan los datos perdiendo su integridad	Significativa Valoración: 3	Limitado Valoración: 2	**Medio Valoración: 6**
	Operaciones de tratamiento que modifican los datos de forma ilegítima	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Máxima Valoración: 4	Significativo Valoración: 3	**Muy Alto Valoración: 12**
Indisponibilidad de los datos	Corte del suministro eléctrico que impide el acceso a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Limitada Valoración: 2	Limitado Valoración: 2	**Medio Valoración: 4**
	Ciberataque que impide acceder a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Significativa Valoración: 3	Significativo Valoración: 3	**Alto Valoración: 9**

- **Riesgo bajo: valores entre 1 y 2**
- **Riesgo medio: valores entre 3 y 6**
- **Riesgo alto: valores entre 7 y 9**
- **Riesgo muy alto: valores entre 10 y 16**

Fuente: construcción propia

Teniendo presente los resultados obtenidos frente al análisis de riesgos, se procede a la construcción de la política ajustada a las necesidades inherentes de la fundación.

7.2 CONSTRUCCIÓN DE LA POLÍTICA

7.2.1 Elementos de la Planeación Estratégica

Para realizar el diagnóstico de una organización desde la planeación estratégica, se consideraron aspectos importantes que permiten realizar una intervención integral frente a sus necesidades.

Se tuvo en cuenta el análisis interno de la organización, desde allí se evaluarán los recursos, capacidades y competencias internas. Esto implica examinar la estructura organizativa, los procesos internos, la cultura corporativa y las habilidades de todas las personas que hacen parte de la Fundación Escuela Contra la Pobreza. También, la identificación de fortalezas y debilidades para reconocer las áreas en las que la organización tiene ventajas competitivas y aquellas en las que presenta oportunidades de mejora. Esto puede incluir aspectos como la calidad de los productos y servicios, la eficiencia operativa, la gestión del talento, la innovación y la protección de datos personales.

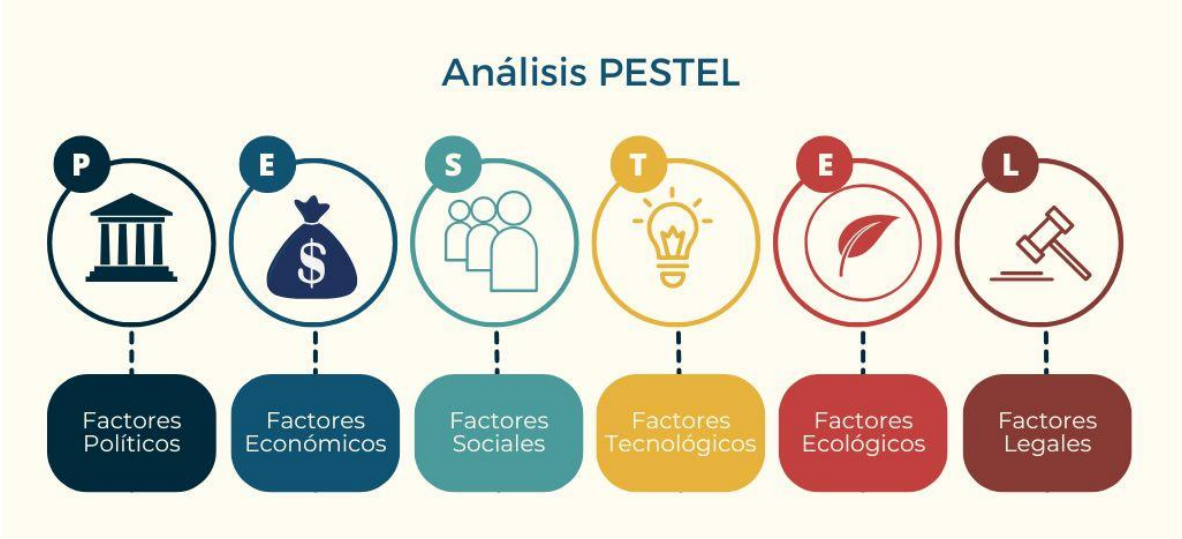
Para el establecimiento de objetivos de manera estratégica, se definirán metas claras y alcanzables de manera que la organización pueda plantearse un plan de trabajo que permita lograrlos en el largo plazo. Estos objetivos deben ser coherentes con la visión y misión de la organización, diseñando planes de acción para alcanzar lo establecido. De esta manera se pueden incluir estrategias de crecimiento, diversificación, novedad en el mercado, la generación de nuevas alianzas estratégicas y la implementación de políticas de protección de datos personales garantizando la seguridad de la información.

Es de resaltar que, para la construcción de la misión y visión de la fundación, fue aplicado un instrumento de recolección de información basado en encuestas, dirigido a los cinco (5) principales lideres. Con sus respuestas y el procesamiento de dicha información

fue desarrollada la propuesta de misión y visión, la cual fue posteriormente discutida y ajustada según los criterios y metas estratégicas deseadas. (anexo 1).

Posteriormente, fue aplicada una matriz PESTEL (Anexo 9) que involucra un análisis externo para identificar el entorno en el que opera la organización. Esto implicara evaluar factores Políticos, Económicos, Sociales, Tecnológicos, Ecológicos y legales que pueden generar un riesgo y afectar su desempeño tal como se puede evidenciar en la figura 3. Finalmente se realizará un proceso de implementación y seguimiento de la política de protección de datos personales para poner en práctica las estrategias y monitorear su progreso, de manera que la información sea de utilidad para la toma de decisiones.

Figura 2Análisis PESTEL.



7.2.1.1 Elementos de la Plataforma Estratégica

De acuerdo con los resultados obtenidos según lo aplicado en el apartado anterior y su respectiva discusión con los líderes de la organización, se plantea de manera definitiva el inicio de la plataforma estratégica que se expone en la tabla 8 a continuación.

Tabla 8Plataforma estratégica desarrollada

Misión: Liderar e impactar positivamente en la población infantil de los barrios marginados de la ciudad de Manizales, para contribuir al bienestar de los individuos y de las comunidades**.**	**Visión:** En 2029, la Fundación Escuela Contra la Pobreza se ve a sí misma como una de las de las organizaciones sin ánimo de lucro que más ha contribuido al mejoramiento de la calidad de vida de los niños marginados de la ciudad de Manizales.
Valores: Honestidad, Excelencia y Carácter	**Principios:** Respeto, Responsabilidad, Creatividad y Compromiso

7.2.2 Política de protección de datos

La fundación escuela contra la pobreza en consideración del cumplimiento de la política de protección de datos, *Habeas Data*, la intimidad y el acceso a la información se compromete a partir de la fecha a realizar el siguiente procedimiento contemplado en el anexo 2.

7.3 PROCEDIMIENTOS Y CONTROLES PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE PROTECCIÓN DE DATOS

7.3.1 Construcción de Elementos del Direccionamiento Estratégico

Para la construcción de la Política de Protección de Datos (anexo2) es importante identificar que la infraestructura de la Fundación Escuela Contra la Pobreza comienza con el organigrama que representa de forma gráfica su estructura, mostrando las relaciones entre sus diferentes partes y las funciones de cada una de ellas. Para este proceso se plantea una actividad con los integrantes de la Fundación para elaborar el respectivo organigrama, acompañado de la documentación pertinente y un cuadro resumen con los perfiles profesionales y personales de los integrantes, para determinar con efectividad cuál será su

respectiva función dentro de la organización. Este procedimiento busca identificar las competencias requeridas para el desarrollo de cada labor al interior de la fundación y la manera en que aporta al logro de sus objetivos estratégicos.

Para el análisis del entorno de la Fundación, la creación de estrategias y el direccionamiento de la organización hacia el alcance de su visión y misión, así como el compromiso con sus valores y objetivos, se aplicaron mecanismos de participación que involucraron a los integrantes de la mesa directiva de la organización, aplicando las siguientes herramientas: El perfil de oportunidades y amenazas en el medio (POAM) (anexo 9); el perfil de capacidad interna de la compañía (PCI) y la matriz de debilidades, oportunidades, fortalezas y amenazas (DOFA) (Anexo 1) (Encinales, 2017).

- El perfil de oportunidades y amenazas en el medio (POAM) es la metodología que permite identificar y valorar las amenazas y oportunidades potenciales de una empresa. Dependiendo de su impacto e importancia, la alta dirección puede determinar si un factor dado en el entorno constituye una amenaza o una oportunidad, para la organización.

Para la elaboración del perfil de oportunidades y amenazas (POAM) se orientará a los integrantes de la fundación a realizar las siguientes acciones:

1. Identifique los asuntos que puedan ser oportunidades o amenazas de la organización (Tormenta de ideas).
2. Agrupe los asuntos por los factores.
3. Identifique los asuntos como oportunidad o amenaza.
4. Califique y priorice la oportunidad o amenaza en la escala: alta, media o baja.
5. Pondere el impacto de la oportunidad o amenaza en el éxito actual del negocio.
6. Interprete la matriz identificando las oportunidades y amenazas de acuerdo con su impacto en el negocio.

7.3.2 Estructuración de Matriz de Riesgos

En la valoración anterior se logra identificar el riesgo que puede sufrir la fundación por no contar con una política de protección de datos que garantice la seguridad de la información, se logra llevar este riesgo a niveles aceptables permitiendo así, presentar como resultado el planteamiento indicado en la Tabla 8, en el cual se evidencia que, en la planeación estratégica y su implementación, son incluidas las políticas de tratamiento de datos personales como estrategia para la organización.

Tabla 9 Matriz de Riesgo Aceptable

Tipo de amenaza	Amenaza	Riesgo	Control	Probabilidad	Impacto	Riesgo residual
Acceso ilegítimo a los datos	Fuga de información	Terceras personas acceden a los datos vulnerado su confidencialidad	Acceso a usuarios autorizados mediante el uso de credenciales y MFA	Despreciable Valoración: 1	Significativo Valoración: 3	**Medio Valoración: 3**
	Operaciones de tratamiento no autorizadas	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Acceso a usuarios autorizados mediante el uso de credenciales y MFA	Despreciable Valoración: 1	Limitado Valoración: 2	**Bajo Valoración: 2**
	Ataque de software malicioso (Ciberataque)	Se modifican los datos perdiendo su integridad	Utilización de sistema antivirus de última generación	Despreciable Valoración: 1	Limitada Valoración: 2	**Bajo Valoración: 2**
Modificación no autorizada de los datos	Operaciones de tratamiento que modifican los datos de forma ilegítima	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Acceso a modificar los datos sólo a los perfiles de usuario autorizados	Despreciable Valoración: 1	Significativo Valoración: 3	**Medio Valoración: 3**

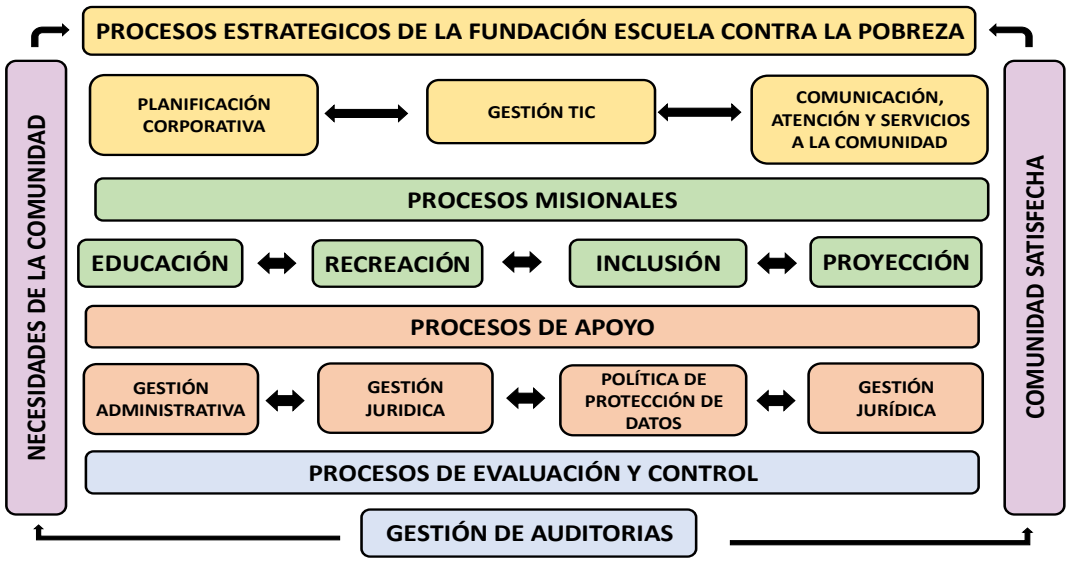
	Corte del suministro eléctrico que impide el acceso a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Utilización de sistemas de alimentación ininterrumpida	Despreciable Valoración: 1	Limitado Valoración: 2	**Bajo Valoración: 2**
Indisponibilidad de los datos	**Ciberataque que impide acceder a los datos**	**Imposibilidad de acceso a los datos porque no están disponibles**	**Utilización de sistema antivirus de última generación**	**Limitada Valoración: 2**	**Significativo Valoración: 3**	**Medio Valoración: 6**

Fuente: construcción propia

7.3.3 Elaboración del Mapa de Procesos

A continuación, se propone el siguiente mapa de procesos (anexo 8) que dé cuenta de las acciones de la fundación Escuela Contra la Pobreza. Es importante mencionar que este se desarrolla con la información obtenida de las matrices anteriormente mencionadas elaboradas en la planeación estratégica.

Figura 3 Mapa de Procesos Fundación Escuela Contra la Pobreza



Fuente: construcción propia

7.3.4 Construcción del Indicador

Se plantean los siguientes indicadores basados en la Norma Técnica Colombiana NTC ISO/IEC 27001 (ISO, 2013) y cumpliendo con lo establecido en la guía de indicadores de gestión para la seguridad de la información del ministerio de la TIC (anexo 3). La Tabla 10 presenta toda la información relativa a la construcción del indicador número 1, relacionado con la organización de seguridad de la información.

Tabla 10 Parámetros de Construcción del Indicador 1, Organización de Seguridad de la Información

<table>
<tr><th colspan="6">INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.</th></tr>
<tr><td colspan="2">IDENTIFICADOR</td><td colspan="4">SGIN01</td></tr>
<tr><th colspan="6">DEFINICIÓN</th></tr>
<tr><td colspan="6">El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad</td></tr>
<tr><th colspan="6">OBJETIVO</th></tr>
<tr><td colspan="6">Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.</td></tr>
<tr><th colspan="6">TIPO DE INDICADOR</th></tr>
<tr><td colspan="6">Indicador de Gestión</td></tr>
<tr><td colspan="2">DESCRIPCIÓN DE VARIABLES</td><td colspan="2">FORMULA</td><td colspan="2">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VSI (Variable de Seguridad de Información)01: Número de personas con su respectivo rol definió según el modelo de operación asignación 2</td><td colspan="2" rowspan="2">(VSI01/VSI02) *100</td><td colspan="2">Capítulo 2 de la guía del modelo de operación del Marco de seguridad y privacidad de la información</td></tr>
<tr><td colspan="2">VSI02: Número de personas con su respectivo rol definió después de un año</td><td colspan="2">Actas de asignación de personal.</td></tr>
<tr><th colspan="6">METAS</th></tr>
<tr><td>MÍNIMA</td><td>75-80%</td><td>SATISFACTORIA</td><td>80-90%</td><td>SOBRESALIENTE</td><td>100%</td></tr>
<tr><th colspan="6">OBSERVACIONES</th></tr>
<tr><td colspan="6">De acuerdo con lo establecido en el capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información, es necesario crear nuevos cargos y asignar responsabilidades en los actuales, por lo tanto, el indicador está enfocado, no solo a la contratación de nuevas personas, sí no a la asignación de responsabilidades.</td></tr>
</table>

Fuente: elaboración propia

En el indicador número 2, cuyos parámetros de construcción se presentan en la Tabla 11, se encuentra la Variable de Seguridad de Información -VSI- la cual es usada para determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a lo relacionado

con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad.

Tabla 11 Parámetros de Construcción del Indicador 2, Cubrimiento del SGSI en Activos de Información

INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.	
IDENTIFICADOR	SGIN02
DEFINICIÓN	
El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos **críticos** de información de una entidad y los controles aplicados.	
OBJETIVO	
Hacer un seguimiento a la inclusión de nuevos activos críticos de información y su control, dentro del marco de seguridad y privacidad de la información.	

INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI 3: Número de activos críticos de información incluidos en el alcance de implementación del modelo, incluidos en la zona de riesgo inaceptable y la implementación del control no requiere adquisición de elementos de hardware o software.		(VSI3/VSI4) *100		Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos	
VSI 4: Número de activos críticos de información incluidos en el alcance de implementación del modelo; activos incluidos en la zona de riesgo inaceptable.				Inventario de Activos de información, nuevos	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80-90%	**SOBRESALIENTE**	00%
OBSERVACIONES					
El indicador de cada proceso debe ser recolectado y promediado para construir un indicador que refleje el estado a nivel empresa. El terminó "incluir un activo" debe ser entendido como realizar la correcta clasificación del activo, tratamiento, evaluación de riesgos sobre el mismo y determinación de controles para minimizar el riesgo calculado. Para este indicador, solo se tienen en cuenta los controles que no implican adquisición de hardware o software.					

7.3.5 Capacitación y Formación

Se capacito a los voluntarios y lideres con un total de 16 personas en las dos capacitaciones de la Fundación sobre cómo se debe llevar la protección de datos personales de cada uno de los usuarios, como también en el manejo de indicadores y *disclairmer* (anexo 4, 5,6 y 7), realizando la salvedad de la consecuencia legal y económica de un indebido manejo.

Foto 1 Capacitación Habeas Data Voluntarios

Foto 2 Capacitación política de tratamiento de datos lideres de la fundación

8 CONCLUSIONES

- Se realizó un diagnóstico a la planeación estratégica de la Fundación Escuela Contra la Pobreza y desde el enfoque de algunos elementos de la misma se identificaron algunas fortalezas como es el caso de la conexión con la población vulnerable, el conocimiento de la zona de enfoque para realizar las actividades, lo que permitió identificar las áreas de mejora dentro de la organización, tales como el grupo de lideres voluntarios de recreación, los cuales, se les sensibilizo en el principio de realidad de cada grupo que se trabaja y el lenguaje que se debe utilizar y limites que deben plantear. El análisis interno evaluó recursos, capacidades, competencias y procesos, destacando la importancia de una gestión eficiente del talento, innovación y protección de datos personales. A través de la formulación de objetivos estratégicos claros, se establecieron planes de acción que están alineados con la misión y visión de la organización y de igual forma se definieron los valores y principios organizacionales, los cuales se diseñaron en conjunto con los líderes de la Fundación y esto favorecerá no solo el compromiso de los mismos sino también el crecimiento sostenible de la organización.

- El análisis externo mediante la matriz PESTEL permitió identificar factores del entorno que podrían influir en el desempeño de la Fundación, proporcionando una base para mitigar riesgos poténciales como la falta de planeación de actividades y retraso en la toma de decisiones. La implementación de políticas, como la protección de datos, y el seguimiento de su progreso garantizan que la organización esté mejor preparada para adaptarse a los cambios del entorno y continuar su misión social de manera sostenible y segura. Esto favorece la toma de decisiones informada y alineada con los objetivos a largo plazo de la organización.

- La elaboración de la Política de Protección de Datos para la Fundación Escuela Contra la Pobreza se fundamenta en un análisis integral de la estructura organizativa y el entorno de la misma. A través de la creación del organigrama y la evaluación de

las competencias de su personal, se tuvo como objetivo alinear las funciones de los miembros con los objetivos estratégicos de la organización. Además, el uso de herramientas de análisis como el POAM y la matriz DOFA permitió identificar oportunidades como la credibilidad que tiene la Fundación en la ciudad por su labor. En cuanto a las principales amenazas se encuentran los limitados recursos que tienen para el desarrollo de sus actividades, así como los riesgos asociados a la protección de la información y de los datos que manejan, lo cual les podría generar sanciones económicas considerables.

- Este enfoque de algunos elementos estratégicos permitió fortalecer la capacidad de la Fundación para gestionar sus recursos y cumplir con su misión, y además deja explícita la necesidad de la protección de la información en su operación diaria. La estructuración de una política de tratamiento de datos personales permite mitigar riesgos potenciales y favorecer un manejo adecuado de la información, así como la seguridad y confidencialidad en el marco de la nueva era digital. Esto consolida algunos elementos de la planeación estratégica de la organización y le permite las herramientas necesarias para adaptarse a su entorno y maximizar su impacto social.

- Se estructuró una matriz de riesgo en la cual se plantean 6 preguntas y se evalúa su probabilidad, riesgo, impacto, con el fin de identificar y evaluar la probabilidad e impactos negativos derivados de que una amenaza se potencialice, el análisis de riesgos tiene como objetivo establecer las acciones que prevengan, reduzcan o eviten en la medida de lo posible el surgimiento de esas amenazas y que permita minimizar a un nivel aceptable la exposición a los riesgos, por lo cual, se añadió una segunda matriz, en la que, debido a la implementación de la política de protección de datos, se validó la mitigación efectiva de los riesgos identificados.

- La construcción de la Política de Protección de Datos para la Fundación Escuela Contra la Pobreza se fundamenta en un análisis detallado de su estructura organizativa y el entorno en el que opera. La estructuración del organigrama, junto

con la identificación de los perfiles profesionales y competencias de los integrantes de la Fundación, es esencial para alinear sus funciones con los objetivos estratégicos de la organización. Este proceso ayuda a que cada miembro contribuya de manera efectiva al logro de la misión y visión de la Fundación, lo cual no se tenía antes debido principalmente a la ausencia de roles claros en cada proceso.

- El uso de herramientas estratégicas como el POAM y la matriz DOFA permitió a la Fundación identificar tanto las oportunidades como las amenazas que podrían impactar su desempeño. Este análisis participativo y colaborativo con la mesa directiva no solo facilitó la identificación de riesgos, sino que también fortalece la toma de decisiones y la planificación futura. La implementación de estas herramientas permite que la Fundación esté mejor preparada para enfrentar desafíos y aprovechar las oportunidades de manera estratégica y coherente.

- Se estructuró un mapa de procesos con una estructura integral y consolidada, que articula los procesos estratégicos, misionales, de apoyo y de evaluación de la institución. Cada uno de estos componentes está diseñado para responder a las necesidades de la comunidad y garantizar su satisfacción, estableciendo un enfoque claro hacia la gestión efectiva de los recursos y las actividades, este mapa fue desarrollado durante la consultoría con la participación de lideres y voluntarios de la misma, donde se destaca el rol de los lideres desde su presencia permanente y activa en la fundación.

- Los procesos estratégicos, como la planificación corporativa, la gestión de TIC y la comunicación con la comunidad, se alinean con los objetivos misionales de la Fundación, que abarcan áreas clave como la educación, recreación, inclusión y proyección. Estos a su vez son respaldados por procesos de apoyo que aseguran un manejo adecuado en la gestión administrativa, jurídica y, particularmente, la política de protección de datos, un aspecto fundamental en la era digital.

- El componente de evaluación y control, mediante la gestión de auditorías, garantiza que todos los procesos se realicen de manera efectiva y que la Fundación se mantenga alineada con sus metas estratégicas, permitiendo una mejora continua y favoreciendo los impactos positivos en la comunidad. Este enfoque integral refuerza la sostenibilidad y el crecimiento de la organización, maximizando su capacidad para cumplir su misión.

- La implementación de indicadores basados en la Norma Técnica Colombiana NTC ISO/IEC 27001 y las directrices del Ministerio de TIC resalta la importancia de una gestión sistemática y efectiva de la seguridad de la información dentro de la Fundación Escuela Contra la Pobreza. La adopción de un enfoque estratégico para el seguimiento y control de estos indicadores permitirá a la Fundación optimizar su capacidad de respuesta ante amenazas a la seguridad, mejorar la gestión de sus activos y asegurar la continuidad de su misión social en un entorno cada vez más digital y vulnerable.

- El primer indicador de seguridad de la información que fue establecido, permite evaluar el compromiso de la alta dirección con la asignación de recursos humanos y responsabilidades clave en este ámbito. A través de un seguimiento de las personas involucradas en la gestión de la seguridad de la información, se puede medir el progreso hacia una estructura organizativa más robusta y consciente de la protección de los datos. El segundo indicador por su parte está centrado en el cubrimiento del Sistema de Gestión de Seguridad de la Información (SGSI) en activos críticos, asegura que los controles adecuados sean aplicados a los activos de información de mayor riesgo, y minimiza las vulnerabilidades sin requerir inversiones adicionales en hardware o software. Estos indicadores no solo proporcionan un marco de evaluación continua, sino que también ayudan a mitigar riesgos y fortalecer la infraestructura de seguridad de la información de la fundación, garantizando la protección de los datos personales y la estabilidad operativa de la organización.

9 REFERENCIAS BIBLIOGRÁFICAS

Agencia Española Protección Datos (2021). Gestión del riesgo y evaluación de impacto en tratamiento de dato. Disponible en: https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Bedoya, C. A. (2014). Solución informática de gestión de datos personales del ciudadano colombiano. Tesis de maestría, Universidad Javeriana. Repositorio institucional de la Universidad Javeriana. Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/15074/CamargoBedoyaCarlosAndres2014.pdf?sequence=3

Beltrán, J.M.(2005) INDICADORES DE GESTION, Herramienta para lograr la competitividad. 3R editores. Disponible en : https://www.economicas.unsa.edu.ar/afinan/informacion_general/book/manual_indicadores.pdf

Congreso de la República (2008). Ley 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos. Bogotá, Colombia: Diario Oficial 47219 de diciembre 31 de 2008. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34488

Congreso de la República (2012). Ley Estatuaria 1581 del 2012, de 17 de octubre. Publicado en Diario Oficial 48587 de octubre 18 de 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

Congreso de la República (2012). Ley Estatuaria 1581 del 2012, de 17 de octubre. Artículo 2. Publicado en Diario Oficial 48587 de octubre 18 de 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

Congreso de la República (2012). Ley Estatuaria 1581 del 2012, de 17 de octubre. Artículo 3, literal g. Publicado en Diario Oficial 48587 de octubre 18 de 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

Congreso de la República (2012). Ley Estatuaria 1581 del 2012, de 17 de octubre. Artículo 5. Publicado en Diario Oficial 48587 de octubre 18 de 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República (2012). Ley Estatuaria 1581 del 2012, de 17 de octubre. Artículo 17, literal k. Publicado en Diario Oficial 48587 de octubre 18 de 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

Congreso de la República (2012). Ley Estatuaria 1581 del 2012, de 17 de octubre. Artículo 23. Publicado en Diario Oficial 48587 de octubre 18 de 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Constitución política de Colombia. Artículo 2. 7 de julio de 1991 (Colombia). Disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2001/0219.pdf

Constitución política de Colombia. Artículo 6. 7 de julio de 1991 (Colombia). Disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2001/0219.pdf

Constitución política de Colombia. Artículo 15. 7 de julio de 1991 (Colombia). Disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2001/0219.pdf

Corte Constitucional de Colombia (2011). Sentencia 748 DE 2011, 6 de octubre. Relatoría corte constitucional de Colombia. Disponible en: https://www.corteconstitucional.gov.co/relatoria/2011/C-748-11.htm

Departamento administrativo de la Función Pública (2016). Instructivo de la política para Tratamiento de Datos Personales. Disponible en: https://www.funcionpublica.gov.co/documents/418537/1512450/Instuctivo+de+la+Pol%C3%ADtica+para+el+Tratamiento+de+Datos+Personales.pdf/f7d7cbe2-6739-46de-9f76-ee147cf1aa60?download=true

Duran Cardo, A. B. (2015). La figura del responsable en el derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel. Tesis doctoral, Universidad Autónoma de Barcelona. Repositorio institucional de la Universidad Autónoma de Barcelona. http://hdl.handle.net/10803/319454

Laudon, J.P; e Laudon, K.C. (2016). Sistemas de información gerencial. Decimocuarta edición. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gc.scalahed.com/recursos/files/r161r/w25735w/ld-Sistemas_de_informacion_gerencial_14%20edicion.pdf.

Miguel, P. (2015). Seguridad en los sistemas informáticos. España: RA-MA. Disponible en: https://www.google.com.co/books/edition/Protecci%C3%B3n_de_Datos_y_Seguridad_de_la_I/8aa6EAAAQBAJ?hl=es-419&gbpv=1&pg=PA7&printsec=frontcover.

Machuca, S. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. Revista Universidad y Sociedad, 14(2), 244-251, 02 de abril de 2022. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202022000200244&lng=es&tlng=es

Ministerios de Tecnología de la Información y Comunicaciones (2021). Anexo 1, Modelo de Seguridad y Privacidad de la Información. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf

Naranjo-Godoy, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador. Foro: Revista de Derecho, (27), 63-82. Disponible en: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2631-24842017000100063&lng=es&tlng=es

Ordóñez, L. (2019). El procedimiento de solicitud de adecuación de los datos de conformidad con la identidad de género. Reflexiones desde el derecho fundamental a la protección de datos. Foro: Revista de Derecho, (32), 179-198. Disponible en: https://doi.org/10.32719/26312484.2019.32.10

Organización Internacional de Normalización. (2013). sistema de gestión de la seguridad de la información (ISO/IEC 27001). Disponible en: https://normaiso27001.es/

(Organización de las Naciones Unidas para la Educación, l. C. *Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura* . Obtenido de https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/#

Ornelas, L. G., e Higuera, M. (2013). La autorregulación en materia de protección: la vida hacia una protección global. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, (9), 2-30.

Presidencia de la República de Colombia (2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá, Colombia: Diario Oficial 48834 de junio 27 de 2013. Recuperado el 10 de octubre de 2022. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=53646

Presidencia de la República (2014). Decreto 886 del 13 de mayo de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

Quiroz, R. (2016). El Hábeas Data, protección al derecho a la información y a la autodeterminación informativa. Letras (Lima), 87(126), 23-27. Disponible en: http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2071-50722016000200002&lang=es

Remolina-Angarita, N. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? International Law, (16), 489-523. Disponible en : http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-81562010000100015&lng=en&tlng=es.

Superintendencia de Industria y Comercio (2012). Cartilla, formatos modelos para el cumplimiento de la obligación establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios. Disponible en: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf.

Superintendencia de Industria y Comercio (2016). Aspectos prácticos sobre habeas data. Bogotá, Colombia. Disponible en: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho_de_Habeas_Data.pdf.

Superintendencia de Industria y Comercio (2022). Manejo de información personal, 'Habeas data. Disponible en: https://www.sic.gov.co/manejo-de-informacion-personal#:~:text=El%20dato%20semiprivado%20es%20aquel,el%20dato%20financiero%20y%20crediticio

Universidad del Rosario (2021). Política de Gestión de Datos e Información Institucional. Dirección de Planeación y Efectividad institucional. Mayo de 2021. Disponible en: https://repository.urosario.edu.co/server/api/core/bitstreams/ce09ece2-45ad-4ba1-bc10-b1c5f9002712/content

10 ANEXOS

Anexo 1 Encuestas Realizada a Lideres de la Fundación Escuela Contra la Pobreza

Anexo 2 Política de Protección de Datos Personales Fundación Escuela Contra la Pobreza

Anexo 3 Guía de Indicadores de Gestión Para la Seguridad de la Información Ministerio de las TIC´S.

Anexo 4 Disclaimer Entrada a Eventos de la Fundación.

Anexo 5 Disclaimer Asistencia

Anexo 6 Disclaimer Autorización Datos Personales Menor de Edad

Anexo 7 Disclaimer Autorización Persona Jurídica

Anexo 8 Mapa de Procesos

Anexo 9 Acta de Realización Matriz PESTEL y POAM