	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	Documento	Código	Fecha	Revisión
	FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	F-AC-DBL-007	10-04-2012	A
Dependencia	Aprobado		Pág.	
DIVISIÓN DE BIBLIOTECA	SUBDIRECTOR ACADÉMICO		1(104)	

RESUMEN – TRABAJO DE GRADO

AUTORES	TANIA TATIANA PACHECO GARCÍA		
FACULTAD	INGENIERÍAS		
PLAN DE ESTUDIOS	INGENIERÍA DE SISTEMAS		
DIRECTOR	YESICA MARÍA PÉREZ PÉREZ		
TÍTULO DE LA TESIS	DISEÑO DE UN MANUAL PARA REDUCIR EL RIESGO DE ATAQUES DE INGENIERÍA SOCIAL SOBRE EL PERSONAL DEL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO ORIENTE SUBSEDE CÚCUTA		
RESUMEN (70 PALABRAS APROXIMADAMENTE)			
<p>COMO UNA ESTRATEGIA SE PLANTEA EL DISEÑO DE UN MANUAL, EN EL CUAL ENCONTRAREMOS UN CONJUNTO DE ACCIONES QUE IMPLEMENTADOS AL INTERIOR DE LA ORGANIZACIÓN, CONTRIBUYE EN EL AUMENTO DE LA EFECTIVIDAD DE LAS CAMPAÑAS DE SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN, ASÍ MISMO SERVIRÁ COMO PUNTO CLAVE DE REFERENCIA PARA EL CUMPLIMIENTO DE ALGUNOS DE LOS NUMERALES DE LA NORMA ISO 27001:2013.</p>			
CARACTERÍSTICAS			
PÁGINAS: 104	PLANOS: 0	ILUSTRACIONES: 29	CD-ROM: 1



**DISEÑO DE UN MANUAL PARA REDUCIR EL RIESGO DE ATAQUES DE
INGENIERÍA SOCIAL SOBRE EL PERSONAL DEL DEPARTAMENTO
ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO
ORIENTE SUBSEDE CÚCUTA**

TANIA TATIANA PACHECO GARCÍA

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2016**

**DISEÑO DE UN MAUAL PARA REDUCIR EL RIESGO DE ATAQUES DE
INGENIERÍA SOCIAL SOBRE EL PERSONAL DEL DEPARTAMENTO
ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO
ORIENTE SUBSEDE CÚCUTA**

TANIA TATIANA PACHECO GARCÍA

**Trabajo de grado presentado como requisito para optar al título de
Ingeniera de Sistemas**

**Director
ESP. YESICA MARÍA PÉREZ PÉREZ**

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2016**

CONTENIDO

	Pág.
INTRODUCCIÓN	11
1. DISEÑO DE UN MANUAL PARA REDUCIR EL RIESGO DE ATAQUES DE INGENIERÍA SOCIAL SOBRE EL PERSONAL DEL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO ORIENTE SUBSEDE CÚCUTA.	13
1.1 PROBLEMA DE INVESTIGACIÓN	13
1.2 FORMULACIÓN DEL PROBLEMA	13
1.3 OBJETIVOS	14
1.3.1 General.	14
1.3.2 Específicos.	14
1.4 JUSTIFICACIÓN	14
2. MARCO REFERENCIAL	16
2.1 ANTECEDENTES	16
2.2 BASES TEÓRICAS	19
2.2.1 Políticas de Seguridad	19
2.2.2 Seguridad Informática	20
2.2.3 Ingeniería Social.	21
2.2.4 Perfil del Atacante	21
2.2.4.1 Fases de la ingeniería social.	22
2.2.5 Técnicas de Ataque.	22
2.2.6 Social Engineering Toolkit (SET).	24
2.2.7 Metasploit framework	24
2.2.8 Familia ISO/IEC 27000Tabla 1. Normas ISO/IEC 27000	25
2.2.9 ISO/IEC 27001:2013	26
2.2.10 ISO/IEC 27002	31
2.2.11 ISO/IEC 27002:2013	32
2.3 MARCO CONCEPTUAL	33
2.3.1 Generalidades	34
2.3.2 Estructura organizacional.	36
2.3.3 Ficha institucional	38
2.3.4 Descripción de las Investigaciones Continuas del DANE en la Subsede de Cúcuta	38
2.4 MARCO LEGAL	70
2.4.1 Leyes informáticas colombianas	70
2.4.2 Ley 603 de 2000.	72
2.4.3 Ley 734 de 2002.	72
2.4.4 Decreto 1377 de 2013.	72
2.4.5 Derechos de autor	72

3. METODOLOGÍA DE LA INVESTIGACIÓN	74
3.1 TIPO DE INVESTIGACIÓN	74
3.2 FUENTES DE INFORMACIÓN	74
3.2.1 Fuentes de información primaria	74
3.2.2. Fuentes de información secundaria	74
3.3 POBLACIÓN Y MUESTRA	74
4. PRESENTACIÓN DE RESULTADOS	75
4.1 REALIZAR UNA AUDITORIA PASIVA PARA IDENTIFICAR FACTORES DE RIESGO QUE EXPONEN A LA INGENIERÍA SOCIAL EN EL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO SUBSEDE CÚCUTA.	75
4.2 IDENTIFICAR LOS OBJETIVOS DE CONTROL Y CONTROLES DE LA 27001 A LOS QUE SE ENCUENTRA EXPUESTOS EL DANE Y PUEDAN SER VULNERADOS POR INGENIERÍA SOCIAL.	80
4.3 DEFINIR LOS CRITERIOS DEL MANUAL DE PREVENCIÓN DE RIESGOS DE ATAQUES DE INGENIERÍA SOCIAL PARA EL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO ORIENTE SUBSEDE CÚCUTA.	83
5. CONCLUSIONES	98
BIBLIOGRAFÍA	99
ANEXOS	100

LISTA DE FIGURAS

	Pág.
Figura 1. Modelo de McCumber	20
Figura 2. Proceso de Gestión de Riesgo	29
Figura 3. Dominios de la norma ISO/IEC 27001:2013	31
Figura 4. Objetivos de la Seguridad de la Información	32
Figura 5. Organigrama	36
Figura 6. Diagrama de Contexto GEIH	40
Figura 7. Diagrama de Contexto CEED	42
Figura 8. Diagrama de Contexto ENA	43
Figura 9. Diagrama de Contexto EEVV	46
Figura 10. Diagrama de Contexto EAI	51
Figura 11. Diagrama de Contexto ECA	52
Figura 12. Diagrama de Contexto EDIT	53
Figura 13. Diagrama de Contexto MMM	55
Figura 14. Diagrama de Contexto EDI	56
Figura 15. Diagrama de Contexto ICCP	57
Figura 16. Diagrama de Contexto ICCV	58
Figura 17. Diagrama de Contexto ICESP	59
Figura 18. Diagrama de Contexto IPC	60
Figura 19. Diagrama de Contexto IPP	61
Figura 20. Diagrama de Contexto IPVN	62
Figura 21. Diagrama de Contexto MICRO	63
Figura 22. Diagrama de Contexto EAS	64
Figura 23. Diagrama de Contexto MTS	65
Figura 24. Diagrama de Contexto ECSC	66
Figura 25. Diagrama de Contexto ESAG	67
Figura 26. Diagrama de Contexto ETUP	68
Figura 27. Diagrama de Contexto ELIC	69
Figura 28. Diagrama de Contexto EAM	69
Figura 29. Diagrama de Contexto MMH	70

LISTA DE TABLAS

	Pág.
Tabla 1. Normas ISO/IEC 27000	25
Tabla 2. Contenido ISO 27001:2013	27
Tabla 3. Controles del Anexo A	31
Tabla 4. Puntos de la Norma	32

LISTA DE GRAFICAS

	Pág.
Grafica 1. Pregunta. N° 1 - Encuesta Seguridad de la Información	75
Grafica 2. Pregunta. N° 3 - Encuesta Seguridad de la Información	76
Grafica 3. Pregunta. N° 6 - Encuesta Seguridad de la Información	77
Grafica 4. Pregunta. N° 10 - Encuesta Seguridad de la Información	77
Grafica 5. Pregunta. N° 13 - Encuesta Seguridad de la Información	78
Grafica 6. Pregunta. N° 14 - Encuesta Seguridad de la Información	78
Grafica 7. Pregunta. N° 18 - Encuesta Seguridad de la Información	79

INTRODUCCIÓN

Las ciencias computacionales han avanzado a pasos agigantados en las últimas décadas, trayendo con ello el progreso de la informática, los sistemas, las telecomunicaciones, y otras aplicaciones de tecnología, forjando la modernización de la sociedad en todos los ámbitos y sentidos, haciendo especial énfasis en las empresas y su continuidad en el negocio, relacionándolas íntimamente con la tecnología de información y la evolución en la sistematización de sus procesos, así como la interacción de diferentes factores, tales como talento humano, recursos tecnológicos, financieros entre otros, que administrados de manera coordinada derivan bienes y servicios que les permite competir y mantenerse en un mercado laboral tan exigente como el actual, donde sus tendencias cada día son mayores.

El avance tecnológico no solo se ha visto aplicado en equipos de última generación, sino que también ha impactado la productividad de las organizaciones actuales, al permitirles interconectar todos los sistemas de la organización, para una mayor eficacia en la comunicación y velocidad de respuesta ante los cambios externos. Esta interconexión aunque abre grandes posibilidades de expansión y crecimiento organizacional, también trae consigo nuevos retos y amenazas en la seguridad de la información. Amenazas que han conllevado a que las empresas día a día reglamenten, documenten y evalúen los niveles de seguridad de procesos y procedimientos de la estructura interna, con el objeto de protegerla de ataques externos o en su efecto también internos.

Por lo cual, es necesario sensibilizar a los usuarios para que incorporen buenas prácticas para proteger el entorno de información, y prevenir aún más la posibilidad de formar parte del conjunto que engloba a las potenciales y eventuales víctimas de cualquiera de las amenazas, que constantemente buscan sacar provecho de las debilidades humanas. Pero para ello inevitablemente se deben conocer los peligros latentes, y cómo detenerlos a través de mecanismos de prevención¹.

El presente proyecto “Diseño de Manual para Reducir el Riesgo de Ataques de Ingeniería Social Sobre el Personal del Departamento Administrativo Nacional de Estadística Territorial Centro Oriente Subsede Cúcuta”, pretende exponer medidas de seguridad tendientes a minimizar el volumen de “potenciales víctimas”, brindando herramientas preventivas para el uso de cada una de las tecnologías y servicios más populares y más utilizados por los usuarios y aborda en cada punto los mecanismos de prevención que permitan detectar, de manera temprana y sin acciones complejas, las acciones maliciosas más comunes de la ingeniería Social.

La monografía está estructurada en cuatro capítulos.

El Capítulo I, presenta el planteamiento del problema, Formulación del Problema, Objetivo General y Específicos, y Justificación.

¹ <http://windowsupdate.microsoft.com>

En el Capítulo II, encontramos el Marco Referencial, que contiene: Antecedentes del proyecto, Marco Histórico, Marco Conceptual, y Marco Legal.

El Capítulo III, Se aborda el enfoque metodológico contiene: Tipo de Investigación, Población y Muestra, Técnicas e Instrumentos de Recolección de la Información.

En el Capítulo IV, se presenta el desarrollo del Proyecto.

1. DISEÑO DE UN MANUAL PARA REDUCIR EL RIESGO DE ATAQUES DE INGENIERÍA SOCIAL SOBRE EL PERSONAL DEL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO ORIENTE SUBSEDE CÚCUTA.

1.1 PROBLEMA DE INVESTIGACIÓN

El Departamento Administrativo Nacional de Estadística - DANE, adelanta en el territorio nacional una serie de encuestas que permite recolectar información sobre la fuerza de trabajo, (empleo, desempleo, e inactividad), ingresos y otras variables importantes como características generales y educación de los miembros que conforman cada uno de los hogares seleccionados para tal fin de los diferentes estratos socioeconómicos.

De acuerdo con la ley 0079 de octubre de 1993, en su artículo 5, referencia que los datos suministrados al Departamento Administrativo Nacional de Estadística - DANE, en el desarrollo de los censos y encuestas, no podrán darse a conocer al público ni a las entidades u organismos oficiales, ni a las autoridades públicas, si no únicamente en resúmenes numéricos, que no hagan posible deducir de ellos información alguna de carácter individual o cualquier otro del propiamente estadístico.

Lo anterior permite inferir que el activo más valioso para la entidad son los datos suministrados por cada uno de los hogares seleccionados como fuente de recolección. Por lo cual, constantemente realiza inversiones en seguridad de la información para la plataforma tecnológica, dejando a un lado el factor humano, que hace parte de los 3 pilares a resguardar dentro de la seguridad de la información.

Actualmente el talento humano se presenta como el eslabón débil a la hora de proteger la información, convirtiendo a las personas en el objetivo principal de la ingeniería social a la hora de querer comprometer el activo más valioso de la organización, desvelando información privada de los hogares o incluso realizando acciones perjudiciales para ellos mismos.

El manejo de la información de modo eficiente constituye una de las principales preocupaciones dentro de la entidad, por lo que se hace necesario manejarla y emplearla con mucho criterio, ya que de ello podría depender, en gran medida, el éxito o fracaso de la misma. Es por ello que se pretende diseñar y socializar un manual de buenas prácticas de seguridad de la información para mitigar el impacto de la ingeniería social en la organización.

1.2 FORMULACIÓN DEL PROBLEMA

¿Educar el talento humano de la entidad, en buenas prácticas de seguridad de la información, reduciría el riesgo de ser víctimas de ataques de Ingeniería Social?

1.3 OBJETIVOS

1.3.1 General. Diseñar un manual que permita reducir el riesgo de ser víctimas de ataques de ingeniería social, al personal del Departamento Administrativo Nacional de Estadística Territorial Centro Oriente Subsele Cúcuta.

1.3.2 Específicos. Realizar una auditoria pasiva para identificar factores de riesgo que exponen a la ingeniería social en el departamento administrativo nacional de estadística territorial centro subsele Cúcuta.

Identificar los objetivos de control y controles de la norma ISO 27001:2013 a los que se encuentra expuestos el DANE y puedan ser vulnerados por ingeniería social.

Definir los criterios del manual de prevención de riesgos de ataques de ingeniería social para el Departamento Administrativo Nacional de Estadística Territorial Centro Oriente Subsele Cúcuta.

1.4 JUSTIFICACIÓN

El Departamento Administrativo Nacional de Estadística, invierte en tecnología para prevenir la mayoría de ataques externos, pero prevenir ataques de ingeniería social en el ámbito tanto interno como externo ya que hay muchas que tienen fuentes externas, le resulta un poco más complejo; como un medio para reducir su impacto se plantea sensibilizar constantemente al talento humano, concientizarlo realmente de lo que implica para la entidad y para sí mismo la pérdida de información confidencial. Por lo que resulta importante tener claro algunos conceptos que ayuden a identificar los ataques, los delincuentes, los medios utilizados para extraer datos y por supuesto ejemplos que hagan más palpable y real la Ingeniería Social en nuestro medio y diario vivir.

Como una estrategia se plantea el diseño de un manual de buenas prácticas para la seguridad de la información, en el cual encontraremos un conjunto de acciones que implementados al interior de la organización, contribuye en el aumento de la efectividad de las campañas de sensibilización en seguridad de la información, así mismo servirá como punto clave de referencia para el cumplimiento de algunos de los numerales de la norma ISO 27001:2013, la cual brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI).

La norma ISO 27001:2013 se compone de una serie de requerimientos que proponen un enfoque basado en procesos, y estos últimos en el modelo PHVA (Planear, Hacer, Verificar y Actuar). En el literal 5.2.2 de la norma hace referencia a la formación, toma de conciencia y Competencia, y describe que la organización debe asegurar que todo el personal apropiado tiene conciencia de la pertinencia e importancia de sus actividades de seguridad de la información, así mismo a la contribución al logro de los objetivos de SGSI.

La sensibilización en seguridad de la información, a través de un manual de buenas prácticas de seguridad de la información, sería de vital importancia para mitigar el impacto de la ingeniería social en la empresa, manteniendo el entorno protegido de las amenazas que rodean su activo más relevante (información).

2. MARCO REFERENCIAL

2.1 ANTECEDENTES

A nivel nacional se han desarrollado innumerables estudios, proyectos, manuales, guías, artículos, etc, sobre seguridad informática e ingeniería Social, entre los cuales es preciso destacar los siguientes:

INGENIERIA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero. Luis Eduardo Patiño Durán. Universidad Pontificia Bolivariana, Bucaramanga, Colombia.

Resumen. Cualquiera que sea la actividad o ubicación en la empresa, el trabajo de cada empleado llega a los clientes en forma de servicios; dicho servicio se basa en atributos y lo convierten en una guía para orientar los modos de actuación de cada uno de los colaboradores, frente a clientes y compañeros. Con la actualización de la banca que va de la mano con la globalización y las nuevas tecnologías, se han diversificado los canales transaccionales, condición que aumenta los riesgos de la seguridad y crea nuevos escenarios para cometer delitos financieros. Para prevenir la mayoría de ataques externos se invierte en tecnología, pero prevenir ataques internos de ingeniería social resulta un poco más complejo para cualquier organización; una posible solución es capacitar constantemente a los colaboradores, concientizarlos, sensibilizarlos realmente de lo que implica para la entidad y para sí mismo la pérdida de información confidencial. Entonces, resulta importante conocer algunos conceptos que ayuden a identificar los ataques, los delincuentes, los medios utilizados para extraer datos y por supuesto ejemplos que hagan más palpable y real la Ingeniería Social en nuestro medio y diario actuar. Al final del documento se darán algunas recomendaciones para evitar ser víctimas de este tipo de ataques.

Guías Prácticas para Uso de Técnicas de Ingeniería Social con la Herramienta Set Incluida en la Distribución Backtrack 4 R2. Carmen Lucia Pedraza Garzón, Viviana Andrea Caviedes Figueroa. Corporación Universitaria Minuto De Dios. Bogotá, Colombia 2011.

Resumen. En la actualidad la seguridad informática se ha convertido en un tema importante de ámbito tecnológico. Por ello, se busca cuidar en un mayor nivel la información personal y empresarial, se han identificado distintos tipos de ataques, para conseguir información sensible. La ingeniería social es sin duda la técnica más que poderosa para lograr este cometido, ya que a través de manipulación y engaños se logra que un usuario autorizado revele información que compromete al sistema. Para realizar este tipo de ataques de SET, que es un kit de herramientas diseñado específicamente para realizar ataques de ingeniería social, su objetivo principal es hacer que el usuario sea tentado a realizar una acción necesaria para dañar el sistema, como por ejemplo abrir un archivo adjunto o abrir una página web aparentemente legítima, pero en realidad es falsa.

En el presente documento se analiza la importancia de la seguridad de la información, basada en el factor humano como mayor vulnerabilidad y proponiendo acciones para contrarrestar la ingeniería social.

Guía de Buenas Prácticas de Seguridad de la Información en Contextos de Micro, Pequeñas y Medianas Empresas De La Región. Gerardo Ayala González Julián Alberto Gómez Isaza, Universidad Tecnológica de Pereira, 2011.

Resumen. Este documento se centra en la aplicación de la norma ISO/IEC 27001 en la Implementación y Operación de un Sistema de Gestión de la seguridad de la información (por sus siglas, SGSI), identificando las acciones de: la gestión apropiada, prioridades y responsabilidades de la gerencia en la creación de políticas que garanticen el cumplimiento de los objetivos del SGSI, además se hace referencia a la creación de planes de acción para el tratamiento, análisis y gestión de los riesgos implementando procedimientos que brindan una atención oportuna a los incidentes de seguridad de la información, acompañados de estrategias de capacitación y formación para los integrantes de la organización.

Buenas prácticas en seguridad informática. Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica martes 30 de junio de 2009.

Resumen. Con el objetivo de prevenir la pérdida de datos y otros incidentes que afectan a la seguridad informática dentro de las empresas, el equipo de especialistas de ESET Latinoamérica ha elaborado la Guía del Empleado Seguro, documento que busca ayudar a los empleados de las organizaciones a implementar buenas prácticas de administración de los datos a partir de una comprensión de la problemática y una descripción de las principales amenazas informáticas.

Checklist de Buenas Prácticas en Departamentos TI. Instituto Nacional de Tecnologías de la Comunicación – INTECO.

Resumen. Este documento contiene un listado de tareas o actividades básicas que debemos aplicar en nuestro departamento de TI, para mejorar la gestión de los servicios que prestemos, incrementar la seguridad y garantizar la continuidad de la organización en aspectos tecnológicos.

El uso de la expresión Ingeniería Social, tuvo sus inicios en 1894 con un ensayo del empresario y filántropo holandés J.C. van Marken,² difundido en Francia por Emile Cheysson -uno de los integrantes del Musée social.³ El concepto recibió su mayor impulso en EEUU a través de "Social Engineering", un libro del moderado reformista social estadounidense W. H. Tolman⁴ -conocido en aquella época por "su trabajo para ayudar a

² Nederlandsch Economisch-Historisch Archief: J.C. van Marken - Biografisch portret

³ bio en Wiki francesa: Émile Cheysson

⁴ William Howe Tolman-1909: Social Engineering

los pobres".⁵ La idea central de todo lo anterior era que no había -en las industrias- una función "social" paralela a la de los conocimientos técnicos -algo así como lo que en la actualidad se llama Gerencia de personal o Recursos humanos-. Tratar con los seres humanos, resolución de problemas dentro del (y quizás en todo) lugar de trabajo, es tan importante para las empresas privadas como la utilización óptima de materiales y maquinarias, en términos de eficiencia y rentabilidad debido a factores de motivación y lealtad entre los trabajadores. Se ha sugerido⁶ que los planteamientos de Van Marken, Cheysson y Tolman reflejan el encuentro entre el reformismo social y la gestión de negocios dentro de la perspectiva de "la cuestión laboral" de la época, que preveía la solución de problemas sociales como emanando de la acción motivada por la implementación racional del interés de los actores sociales. Y que ese paralelismo funcional establecido por ellos, haciendo hincapié en el carácter no técnico de las calificaciones profesionales del ingeniero social, incluyendo los talentos del diplomático, está en contraste con el uso posterior del término, basado en la metáfora de la máquina que se convirtió en el núcleo del concepto peyorativo actual- que se popularizó a partir de 1911.

En otras palabras, se sugiere que el origen del término está en el concepto de filantropía tal como fue entendido por los pensadores liberales de la segunda mitad del siglo XIX.⁷ Y que en la tentativa de construir los "ingenieros sociales" como un grupo especializado de "intermediarios racionales" entre el capital y el trabajo, sus proponentes fueron crecientemente empujados, buscando un objetivismo científico, a adoptar una posición mecanicista. Para la década del 30 y 40 del siglo XX, el término había caído en desuso en la mayoría de los países.⁸

A partir de esa especialización se generalizó la percepción que la "ingeniería social" puede ser usada como una técnica o método para lograr una variedad de resultados, es decir, la ingeniería social deja de ser un método para implementar la solución de problemas sociales tales como la pobreza y se transforma en un método de manipular la población.

La ingeniería social, la ciencia y arte de hackear a seres humanos, ha aumentado su auge en la última década, gracias al crecimiento de las redes sociales, los correos electrónicos y demás formas de comunicación a través de la nube. En el sector de la seguridad TI, este término se utiliza para hacer referencia a una serie de técnicas que usan los criminales para manipular a sus víctimas con el fin de obtener información confidencial o para convencerlos de realizar algún tipo de acción que comprometa la integridad de su sistema.

La ingeniería social no es una amenaza nueva, ha existido desde el origen de los tiempos. Gracias a ingenieros tan populares como Kevin Mitnick es uno de los ingenieros sociales más famosos, después de haber sido pionero en la idea en los años 1980 y 1990. Su primera

⁵ New York Times: Dr. Tolman Sails on His Mission.

⁶ David Östlund-2007: The Business Career of the Terminology of Social Engineering 1894-1910

⁷ Ann-Katrin Hatje-2007: Female Social Engineering and Its Philanthropic Roots

⁸ Carl Marklund-2007: Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA

estafa de ingeniería social fue manteniendo una conversación con un conductor de autobús para averiguar dónde comprar los clips que los conductores utilizan para marcar el día y la hora en un boleto. Obteniendo la simpatía del conductor, fue capaz de viajar gratis durante meses debido al hecho de que él tenía el mismo clip que los conductores. Luego pasó a llamar a las empresas de telefonía, haciéndose pasar por alguien que necesitaba ciertos códigos para cobrar llamadas de larga distancia a otras empresas, e hizo una gran cantidad de llamadas de larga distancia cobradas en las cuentas de otras personas. El hacerse pasar por otro y ganar la simpatía de los empleados con información le dio lo que necesitaba para llevar a cabo estas operaciones fraudulentas.

Fran Abagnale, por ejemplo, fue uno de los hackers más famosos con sus múltiples identidades y engañando a los usuarios para que le revelasen información esencial para sus estafas. Cabe citar entre otros a los hermanos Badir, tres hombres ciegos israelíes que obtuvieron códigos de acceso telefónico llamando a secretarios, identificándose como ingenieros en el campo. Les dijeron a los secretarios que necesitaban acceso para hacer su trabajo, y luego escribieron los códigos cuando se los dijeron los secretarios o los identificaron cuando las secretarias los pulsaban en sus teléfonos de marcación por tonos, utilizando sus sentidos auditivos intensificados.

Abraham Abdallah utilizó la revista Forbes para encontrar celebridades con elevados patrimonios, y luego envió cartas a agencias de crédito de referencia con membretes corporativos falsos pidiendo más información. Luego utilizó las direcciones, números de seguridad social y otros datos de identificación de estas correspondencias para abrir tarjetas de crédito, obtener acceso a las cuentas bancarias y en general robar las identidades de las personas más ricas. Este es un ejemplo de ingeniería social ya que por sus membretes corporativos, se ganaba la confianza a través de un disfraz, que luego utilizaba para robar dinero.

2.2 BASES TEÓRICAS

Hoy en día existen muchas técnicas y herramientas que de forma relativamente fácil permiten que personas no autorizadas pueda tener acceso a la información sensible de las organizaciones, cuando los controles no están bien implementados logran su objetivo con poco esfuerzo y conocimiento, causando graves perjuicios para la empresa.

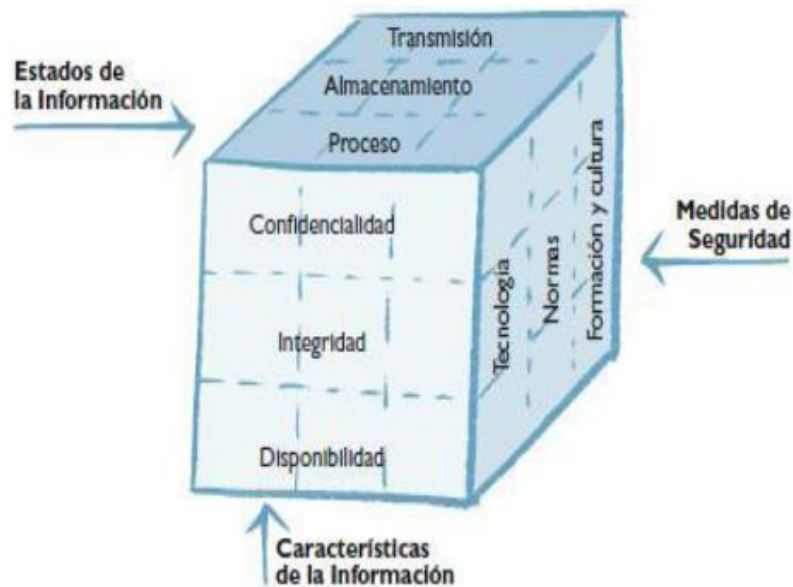
2.2.1 Políticas de Seguridad. Conjunto de requisitos definidos por responsables de un sistema, que indican lo que está o no permitido para mantener segura la información. Igualmente se convierten en medio para concienciar al personal sobre la importancia de la información y servicios críticos que pueden verse afectados por uso inadecuado de los sistemas.

Básicamente, una política de seguridad hace la descripción de lo que se desea proteger y el porqué de ello, cada política es una invitación a reconocer la información como activo principal. Por tal razón, estas deben tener una posición consciente y vigilante del personal en cuanto al uso, limitaciones de los recursos y servicios informáticos, para asegurar los

cuatro aspectos fundamentales de la seguridad información que son: disponibilidad, integridad y confidencialidad.¹⁰

2.2.2 Seguridad Informática. Es un conjunto de procedimientos, actividades, políticas, personas y tecnologías orientadas a disminuir la probabilidad de que se vea comprometida la confidencialidad, integridad y disponibilidad del activo más importante de cualquier organización “la Información”.

Figura 1. Modelo de McCumber



Fuente: Carl Marklund-2007: Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA

Para que un sistema pueda ser definido como seguro garantizar el cuidado de las siguientes características:

- **Integridad:** Se debe garantizar que los datos solo son modificados por personal autorizado como parte de un proceso de negocios legítimo, y que la información procesada es consistentes y confiable.
- **Confidencialidad:** A través de métodos como el cifrado se debe garantizar que la información pueda ser accedida únicamente por usuarios autorizados.
- **Disponibilidad:** los datos deben estar al alcance de los usuarios autorizados para esto en el momento que sean requeridos.

- **No repudio:** Hace referencia a que No se puede negar la autoría, el remitente debe ser quien dice ser. Es decir, un emisor de un mensaje no puede negar que lo generó y viceversa.
- **Trazabilidad** Cuando la información relacionada con las acciones y actividades de los usuarios (personas o procesos) se encuentra debidamente registrada y monitoreada. Adicionalmente, la administración de la seguridad y accesos privilegiados también son monitoreados. La observancia promueve el adecuado funcionamiento de todo el modelo de seguridad informática.
- **Autenticidad:** garantía de que la información es válida y utilizable en tiempo, forma y distribución.

2.2.3 Ingeniería Social. Es un conjunto de técnicas psicológicas y habilidades sociales que permiten que las personas realicen voluntariamente acciones que normalmente no harían. Se vale de errores y fallas en la seguridad informática. Tiene tres tipos; el primero técnicas pasivas como lo es la observación; el segundo, técnicas no presenciales como el uso de teléfono, carta, fax o mail; y el tercero, técnicas presenciales que a su vez tiene dos tipos: las agresivas y las no agresivas. Las agresivas son el uso de suplantación de identidad, extorción o presión psicológica. Y las no agresivas como la búsqueda en la basura (Dumpter Diving), mirar por encima del hombro (Shoulder Sourfing), el seguimiento de personas, entre otras.

Existen herramientas y técnicas creadas con el fin de atraer usuarios a determinadas paginas donde se les ofrece algún producto ilícitamente, otros con el fin de llevarlos engañados a una página web idéntica a la de algún banco, o entidad que permita hacer pagos por internet, donde se solicita al usuario ingresar sus datos personales para utilizarlos de manera ilegal.

Estas herramientas pueden ser usadas para recopilación de información de sospechosos o delincuentes.

2.2.4 Perfil del Atacante. No es fácil identificar un perfil único del delincuente, pero, por lo general en la mayoría de fuentes leídas sobre ingeniería social, dentro de los cuales se encuentran, se pueden mencionar las siguientes características:

- Podría ser un hacker, espía, ladrón o detective privado
- Permanece en calma cuando está al acecho
- Actúa como si perteneciera a la organización
- Estudia a sus víctimas y sabe cómo reaccionaran
- Se retira si observa que algo comienza a fallar
- Si el desafío es muy grande trabaja en equipo

2.2.4.1 Fases de la ingeniería social. Se podrían determinar tres fases en la acción de esta modalidad de fraude:

- **Recopilación de información:** El delincuente hace llamadas telefónicas, envía correos electrónicos e información a través de páginas Web, se cuela en redes sociales y busca información en la basura, entre otros.
- **Selección de la víctima:** El delincuente simula pertenecer a la organización, usa tarjetas de acceso y nombres falsos, busca gerentes de oficinas, subgerentes, asesores, encargados del soporte técnico, recepcionistas, asesores de servicio al cliente y cajeros entre otros, lo que indica que cualquiera puede ser víctima de un ataque de ingeniería social.
- **El ataque:** Se basa en rutas periféricas de persuasión como imposición de autoridad, carisma, reciprocidad, necesidad urgente, validación social o aprovecha la existencia de nuevos productos o servicios para usarlos en su técnica de ataque.

2.2.5 Técnicas de Ataque. Denegación de Servicios: Tiene como objetivo imposibilitar el acceso a los servicios y recursos de una organización durante un periodo indefinido de tiempo. Por lo general, este tipo de ataques está dirigido a los servidores de una compañía, para que no puedan utilizarse ni consultarse, puede afectar a cualquier servidor conectado a internet. Su objetivo no reside en recuperar ni alterar datos, sino en dañar la reputación de las compañías con presencia en internet y potencialmente impedir el desarrollo normal de sus actividades en caso de que éstas se basen en un sistema informático.

A mayoría de los ataques de denegación de servicio aprovechan las vulnerabilidades relacionadas con la implementación de un protocolo TCP/IP modelo.

Generalmente, estos ataques se dividen en dos clases:

- Las denegaciones de servicio por saturación, que saturan un equipo con solicitudes para que no pueda responder a las solicitudes reales.
- Las denegaciones de servicio por explotación de vulnerabilidades, que aprovechan una vulnerabilidades en el sistema para volverlo inestable. Los ataques por denegación de servicio envían paquetes IP o datos de tamaños o formatos atípicos que saturan los equipos de destino o los vuelven inestables y, por lo tanto, impiden el funcionamiento normal de los servicios de red que brindan.

Cuando varios equipos activan una denegación de servicio, el proceso se conoce como “sistema distribuido de denegación de servicio” (DDOS, Distributed Denial of Service).

Fuerza Bruta: Se caracteriza por una tentativa continuada de obtener acceso a un servicio del sistema (ssh, smp, http, etc.), intentando diversas combinaciones de nombre del usuario

y su contraseña. Para llevar a cabo este ataque, el atacante puede usar un software que gestiona diversas combinaciones de caracteres o basarse en una lista de palabras.

En ambos casos un ataque de este género es un ávido consumidor de recursos y potencialmente bastante peligroso, especialmente si los usuarios del sistema no tienen un mínimo de cuidado al elegir sus contraseñas.

MAN IN THE MIDDLE: Es un ataque en donde se intercepta los mensajes en un intercambio de claves públicas y luego se retransmite, sustituyendo su propia clave pública para el atacante, por lo que las dos partes iniciales aun parecen estar comunicándose entre sí.

El ataque debe su nombre al juego de pelota donde dos personas tratan de lanzar un balón directamente el uno al otro, mientras que una persona de entre ellos lo intenta capturar. En un MAN IN THE MIDDLE, el intruso utiliza un programa que parece ser el servidor al cliente y parece ser que el cliente al servidor. El ataque puede ser usado simplemente para tener acceso al mensaje, o permitir el atacante modificar el mensaje antes de retransmitirlo.

DNS Spoofing: Consiste en manipular las direcciones DNS (Domain Name Server) que utiliza el usuario. Los servidores DNS son los encargados de conducir a los usuarios a la página que desean ver. Pero a través de esta acción, los ladrones de datos consiguen que las páginas visitadas no se corresponden con las auténticas, sino con otras creadas para recabar datos confidenciales, sobre todo relacionadas con la banca online.

PHARMING: A través del “pharming” consistente en la manipulación del archivo “host” en computadoras que hacen uso del stack TCP/IP; cuando el usuario teclea en su navegador la dirección de la página a la que quiere acceder, en realidad puede ser enviado a otra creada por el hacker, que tiene el mismo aspecto que la original. Así, el internauta introducirá sus datos confidenciales sin ningún temor, sin saber que los está remitiendo a un delincuente. El pharming puede tener algunas similitudes con las estafas de phishing que se llevan a cabo a través del correo electrónico, aunque las primeras resultan más insidiosas, dado que pueden desviar al usuario a un sitio falso sin que aquel participe o tenga conocimiento de ello.

SPOOFING: Se conoce como la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque es: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado.

BOMBAS LÓGICAS: Ataques con fines maliciosos que se ejecuta un día específico, en una hora específica, etc y que puede ejecutar modificaciones como borrado de un disco duro, entre otras acciones.

WIRELESS CRACK: Ataque usado para crackear contraseñas de redes inalámbricas. Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza

habitualmente con un dispositivo móvil, como un ordenador portátil o un PDA. El método es realmente simple: el atacante simplemente pasea con el dispositivo móvil y en el momento en que detecta la existencia de la red, se realiza un análisis de la misma. Para realizar el wardriving se necesitan realmente pocos recursos. Los más habituales son un ordenador portátil con una tarjeta inalámbrica, un dispositivo GPS para ubicar el PDA en un mapa y el software apropiado.

PHISHING: Un ataque muy simple pero efectivo es engañar al usuario llevándolo a pensar que un administrador del sistema le está pidiendo una contraseña para propósitos legítimos. Quienes navegan en internet frecuentemente reciben mensajes que solicitan contraseñas o información de su tarjeta de crédito con el motivo de crear una cuenta, reactivar una configuración u otra operación aparentemente inofensiva. A este tipo de ataques se lo llama phishing. Los usuarios de estos sistemas deberían ser advertidos temprana y frecuentemente para que no divulguen contraseñas u otra información sensible a personas que dicen ser administradores.

BUFFER OVERFLOW: Es un error de sistema causado por un defecto de programación, de tal forma que el programa que lo sufre pretende escribir más información en el buffer de la que este puede alojar.

Este desbordamiento es posible porque el autor del programa no incluyó el código necesario para comprobar el tamaño y la capacidad del buffer en relación con el volumen de datos que tiene que alojar.

BLIND SQL INJECTION: Ataque a ciegas de inyección de sentencias SQL, usado para explotar las vulnerabilidades de una base de datos que después de ser inyectadas se espera que retorne un error.

SMURF: Ataque de denegación de servicios distribuido, que junto a spoofing busca dejar fuera de servicio un sistema con el uso de grandes paquetes icmp.

2.2.6 Social Engineering Toolkit (SET). Es un kit de herramienta que ayuda en la tarea de realizar ataques de ingeniería social, permite suplantar fácilmente la identidad de un sitio determinado, o enviar ataques por mail a las cuentas de correo de alguna compañía o persona, infectar memorias USB, etc, fue diseñado por David Kennedy (Rel 1K).

Estas herramientas se usan para verificar el nivel de vulnerabilidad de una empresa ante ataques de ingeniería social y para tomar las medidas correspondientes.

2.2.7 Metasploit framework. Es una solución de pruebas de penetración de código abierto desarrollado por la comunidad de Open Source y Rapid⁷. Estándar para pruebas de penetración, con la base de datos publica más grande y de calidad para explotar.

Es la herramienta líder en pruebas de penetración del mundo. Se trata de un proyecto de código abierto que proporciona el software de pruebas de penetración, la información sobre

vulnerabilidades de seguridad, y permite el código de explotación y el desarrollo de firma DS.

El Metasploit Framework, está desarrollado en Ruby con algunos componentes C y assembler, es la plataforma de desarrollo real utilizada para crear herramientas de seguridad de prueba y módulos de explotación, también se puede utilizar como un sistema de pruebas de penetración. Es una herramienta de línea de comandos muy poderosa que ha publicado algunas de las hazañas más sofisticadas a las vulnerabilidades de seguridad pública. También es conocida por sus herramientas antiforenses y de evasión, que se construye en el marco de Metasploit.

2.2.8 Familia ISO/IEC 27000. La familia ISO/IEC 27000 Estándares de seguridad de la información, provee estándares y guías sobre buenas prácticas en sistemas de gestión de seguridad de la información, generalmente aceptadas. En concreto el listado actual de normas que se encuentran en desarrollo y finalizadas son:⁹

Tabla 1. Normas ISO/IEC 27000

ISO/IEC 27000:2009	Proporciona una vista general del marco normativo y un vocabulario utilizado por las normas de la serie.
ISO/IEC 27001:2005	Especificaciones para la creación de un sistema de gestión de la seguridad de la información (SGSI). Publicada en 2005.
ISO/IEC 27002:2005	Código de buenas prácticas para la gestión de la seguridad de la información describe el conjunto de objetivos de control y controles a utilizar en la construcción de un SGSI (actualizada desde la ISO/IEC 17799:2005 y renombrada en el 2007 como ISO 27002:2005). Publicada en 2005 y renombrada en 2007.
ISO/IEC 27003:2010	Directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Es el soporte de la norma ISO/IEC 27001.
ISO/IEC 27004:2009	Describe los criterios de medición y gestión para lograr la mejora continua y la eficacia de los SGSI.
ISO/IEC 27005:2008	Proporciona criterios generales para la realización de análisis y gestión de riesgos en materia de seguridad. Publicada en 2008.
ISO/IEC 27006:2007	Es una guía para el proceso de acreditación de las entidades de certificación de los SGSI.
ISO/IEC 27007	Será una guía para auditar SGSI.
ISO/IEC TR 27008	Proporcionará una guía para auditar los controles de seguridad de la norma ISO 27002:2005.
ISO/IEC 27010	Proporcionará una guía específica para el sector de las comunicaciones y sistemas de interconexión de redes de industrias y Administraciones, a través de un conjunto de normas más detalladas que comenzarán a

⁹ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION ISO/IEC 27000. www.iso27000.es. (Carmen Lucia Pedraza Garzon, 2011)

	partir de la ISO/IEC 27011.
ISO/IEC 27011:27008	Guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051. En España, aún no está traducida.
ISO/IEC 27012	Conjunto de requisitos (complementarios a ISO/IEC 27001) y directrices (complementarias a ISO/IEC 27002) de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.
ISO/IEC 27013	Guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).
ISO/IEC 27014	Guía de gobierno corporativo de la seguridad de la información.
ISO/IEC 27015	Guía de SGSI para organizaciones del sector financiero y de seguros.
ISO/IEC 27031	Guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
ISO/IEC 27032	Será una guía para la cyber-seguridad.
ISO/IEC 27033	Sustituirá a la ISO/IEC 18028, norma sobre la seguridad en redes de comunicaciones.
ISO/IEC 27034	Guía de seguridad en aplicaciones informáticas.
ISO/IEC 27035	Guía de gestión de incidentes de seguridad de la información.
ISO/IEC 27036	Guía de seguridad de outsourcing (externalización de servicios).
ISO/IEC 27037	Guía de identificación, recopilación y preservación de evidencias digitales.
ISO/IEC 27799:2008	Norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.

Fuente: William Hálaby CISSP, 2014. Disponible en: http://isc2capitulocolombia.org/portal/images/documents/ISO_27001-2013_ISC2_Colombia_Chapter.pdf

2.2.9 ISO/IEC 27001:2013¹⁰ Con la norma ISO 27001:2013, se puede demostrar a clientes existentes y potenciales, proveedores y accionistas la integridad de sus datos y sistemas, así como su compromiso con la seguridad de la información. También puede dar lugar a

¹⁰ William Hálaby CISSP, 2014 http://isc2capitulocolombia.org/portal/images/documents/ISO_27001-2013_ISC2_Colombia_Chapter.pdf

nuevas oportunidades de negocio con clientes preocupados por la seguridad; puede mejorar la ética de los empleados y fortalecer la noción de confidencialidad en todo el lugar de trabajo. Además, le permite reforzar la seguridad de la información y reducir el posible riesgo de fraude, pérdida de información y divulgación.

La asociación con SGS para la certificación de seguridad de la información supone un mejor rendimiento de los procesos, talentos cada vez más hábiles y relaciones más sostenibles con los clientes. Tenemos un amplio historial en la realización con éxito de grandes proyectos internacionales. Con presencia en todas las regiones de todo el mundo, nuestro equipo habla el idioma y entiende la cultura de su mercado local.

Tabla 2. Contenido ISO 27001:2013

ISO 27001:2013
0 Introducción
1 Objeto y Campo de Aplicación
2 Referencias Normativas
3 Términos y Definiciones
4 Contexto de la Organización
5 Liderazgo
6 Planificación
7 Soporte
8 Operaciones
9 Evaluación del Desempeño
10 Mejora
A Objetivos de Control y Controles

Fuente: Carl Marklund-2007: Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA

- **Términos y definiciones**

- Todas las definiciones fueron removidas
- Las definiciones relevantes fueron movidas a ISO27000
- Promueve la consistencia de términos y definiciones en toda la familia ISO270XX

- **Contexto de la Organización**

- Relacionados con el contexto de la Organización - determinar los problemas externos e internos.
- Requisito claro para considerar las partes interesadas.
- El contexto determina la política de SI, los objetivos y la forma en que la organización tendrá en cuenta el riesgo y el efecto del riesgo en su negocio.
- Requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios y las obligaciones contractuales.

Contexto Externo

- Social, cultural, político, jurídico, normativo, financiero, tecnológico, económico, natural y ambiente competitivo (internacional, nacional, regional o local)
- Factores clave y tendencias que tienen impacto en los objetivos de la organización
- Relaciones percepciones y valores de los actores externos

Contexto Interno

- Cultura de la organización
- Estructura de gobierno, roles y responsabilidades
- Políticas, objetivos y las estrategias en marcha para alcanzarlos
- Capitales en términos de recursos y de conocimientos (procesos ej., Dinero, tiempo, gente, sistemas y tecnologías)
- Sistemas de información Informales y formales y flujos de procesos para toma de decisiones
- Normas adoptadas, Guías y modelos
- Forma y alcance de las relaciones contractuales
- Relaciones, percepciones y valores de los actores internos

• Liderazgo

- Resume los requisitos específicos para el papel de la alta dirección en el SGSI
- Delinea formas específicas para demostrar la gestión y su compromiso con el sistema.

Ejemplos incluyen:

- Asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles
 - Comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información
- Aunque se renombre la Política del SGSI, los requisitos de política originales permanecen
- La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.

• Planificación

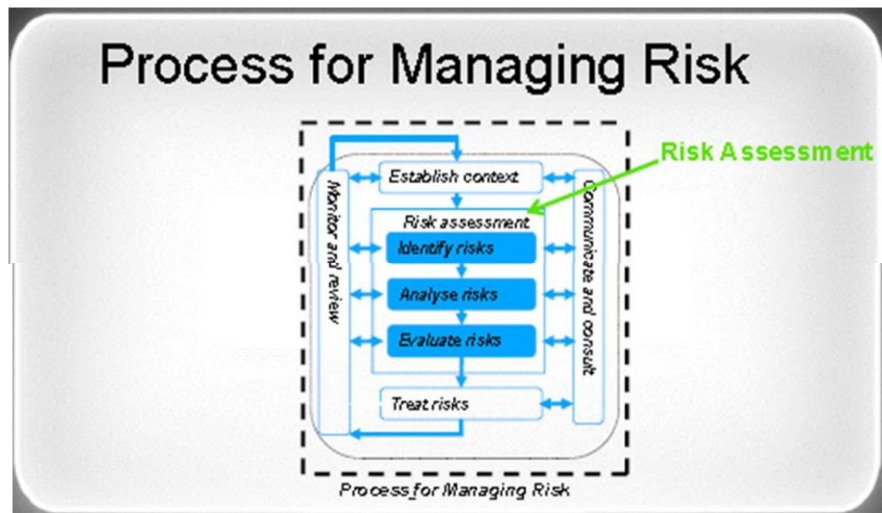
- Establecimiento de objetivos y principios rectores para el SGSI
- Al planificar el SGSI el contexto de la organización debe ser tenido en cuenta a través de la consideración de los riesgos y oportunidades
- Los objetivos de la organización deben estar claramente definidos junto con los planes para alcanzarlos

- Requisitos de evaluación de riesgos más general y alineados con la norma ISO 31000
- Requisitos de la declaración de aplicabilidad (SoA) prácticamente sin cambios.

Riesgo

- Propietario del Riesgo en lugar de propietario del activo
- Sólo es necesario para identificar los riesgos con respecto a Confidencialidad, Integridad y Disponibilidad
- Incluye "riesgos positivos" también conocidos como Oportunidades
- Plan de tratamiento de riesgos usado para crear la declaración de aplicabilidad

Figura 2. Proceso de Gestión de Riesgo



Fuente: Carl Marklund-2007: Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA

Plan de Tratamiento del Riesgo

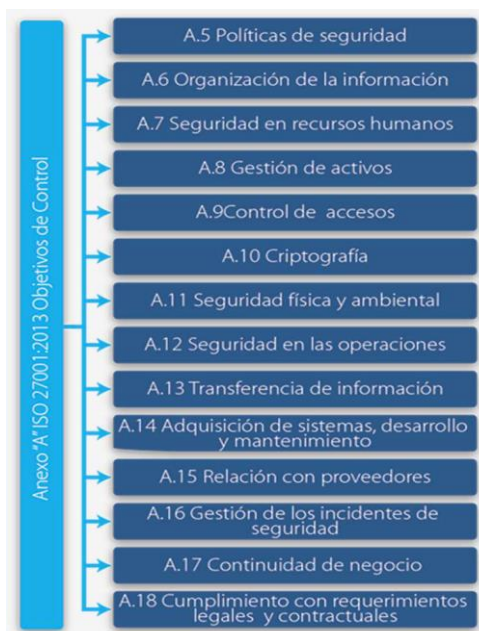
- La cláusula 6.1.3 describe cómo una organización puede responder a los riesgos con un Plan de Tratamiento de Riesgos, una parte importante de esto es la elección de los controles adecuados.
- Estos controles y objetivos de control, figuran en el Anexo A, aunque también es posible, en principio que las organizaciones implementen controles tomados de cualquier otra fuente.

• Soporte

- Lo necesario para establecer, implementar y mantener y mejorar continuamente un SGSI efectivo incluye:
 - Requerimientos de recursos o competencias de las personas involucradas

- Conocimiento y comunicación con las partes interesadas
 - Requisitos para la gestión de documentos
- Se refiere a la "información documentada" en lugar de "documentos y registros"
 - Ya no es una lista de los documentos que se necesitan o nombres particulares que se les debe dar.
 - Más énfasis en el contenido en lugar del nombre.
- **Operaciones**
 - Las organizaciones deben planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información.
 - Se incluye:
 - Llevar a cabo valoraciones de riesgo de SI a intervalos planificados
 - La implementación de un Plan de Tratamiento de Riesgos de SI
- **Evaluaciones del desempeño**
 - Auditorías internas y revisión por la dirección métodos clave de la revisión del rendimiento del SGSI y herramientas para su mejora continua.
 - Requisitos más específicos para la medición de la efectividad.
- **Mejora**
 - Las no conformidades de los SGSI tienen que ser tratadas junto con las acciones correctivas para asegurarse de que no vuelvan a ocurrir.
 - Al igual que con todos los estándares de sistemas de gestión, la mejora continua es un requisito básico de la norma.

Figura 3. Dominios de la norma ISO/IEC 27001:2013



Fuente: Carl Marklund-2007: Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA

Tabla 3. Controles del Anexo A

Control	Descripción
A.6.1.4	Seguridad de la información en la gestión de proyectos
A.12.6.2	Restricciones en la instalación de software
A.14.2.1	Política de desarrollo de seguridad
A.14.2.5	Desarrollo de procedimientos para el sistema
A.14.2.6	Desarrollo de un entorno seguro
A.14.2.8	Sistema de prueba de seguridad
A.15.1.1	Información de seguridad para las relaciones de proveedores
A.15.1.3	Cadena de suministro ICT
A.16.1.4	Evaluación y decisión de los eventos de seguridad de la información
A.16.1.5	Respuesta a incidentes de seguridad de la información
A.17.1.2	Implementación de la continuidad de la seguridad de la información
A.17.2.1	Disponibilidad de las instalaciones para procesamiento

Fuente: Carl Marklund-2007: Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA

2.2.10 ISO/IEC 27002. La ISO 27002, al definirse como una guía protocolar (conjunto de normas a llevar a cabo) en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios:

- **Confidencialidad:** asegurar que, únicamente, personal autorizado tenga acceso a la información.
- **Integridad:** garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas; preservando exactitud y completitud de la misma y de los métodos de su procesamiento.
- **Disponibilidad:** cerciorar que los usuarios autorizados tendrán acceso a la información cuando la requieran y sus medios asociados.

Figura 4. Objetivos de la Seguridad de la Información



Fuente: Carl Marklund-2007: Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA

2.2.11 ISO/IEC 27002:2013. Es el código de prácticas de seguridad de la información el cual tiene como objetivo proveer una guía para la implementación de controles para el Sistema de Gestión de Seguridad de la Información ISO 27001.

Tabla 4. Puntos de la Norma

Política de seguridad	Recomendaciones para el establecimiento de políticas de seguridad de la información para un ISMS.
Organización de Seguridad de la Información	Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
Aspectos organizativos de la seguridad de la información	Organización interna; terceros.
Seguridad de los recursos humanos	Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.

Gestión de Activos	Actividades para el control de activos de información dentro del alcance de un ISMS.
Control de Acceso	Prácticas para el control de acceso a los activos de información o información dentro del alcance de un ISMS
Criptografía	Lineamientos para la protección de la información por medios criptográficos.
Seguridad física y ambiental	Actividades para la prevención de eventos que pueden dañar los activos de información.
Seguridad en las operaciones	Prácticas para asegurar el apropiado control y seguridad sobre los activos de procesamiento.
Seguridad de las Comunicaciones	Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
Adquisición, desarrollo y mantenimiento de Sistemas.	Actividades para el aseguramiento del ciclo de vida desarrollo, mantenimiento o adquisición de sistemas.
Relacionamiento con los Proveedores	Prácticas para la administración de la seguridad de la información con proveedores.
Gestión de Incidentes de Seguridad de la Información	Actividades para la gestión de incidentes de seguridad de la información.
Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios	Actividades para el establecimiento de un plan de continuidad del negocio.
Cumplimiento	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.

Fuente: Carl Marklund-2007: Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA

Los objetivos de control y controles en ISO / IEC 27002:2013 están destinados a ser implementado para cumplir con los requisitos identificados por una evaluación de riesgos.

2.3 MARCO CONCEPTUAL

El Departamento Administrativo Nacional de Estadística (DANE), es la entidad responsable de la planeación, levantamiento, procesamiento, análisis y difusión de las estadísticas oficiales de Colombia.

Pertenece a la rama ejecutiva del estado colombiano, y tiene cerca de 60 años de experiencia. La entidad cumple con los más altos estándares de calidad y ofrece al país y al mundo más de 70 investigaciones de todos los sectores de la economía, industria, población, sector agropecuario y calidad de vida, entre otras.

Toda esta labor, sumada a la aplicación de modernas tecnologías de captura, procesamiento y difusión, así como la calidad humana de todos los que participan en el proceso de la organización, permiten al DANE fortalecer el conocimiento, la confianza y la cultura estadística de los colombianos, reafirmando su condición de rector de las estadísticas en el país.

2.3.1 Generalidades. *Reseña Histórica.* En octubre de 1951 mediante el Decreto 2240, se separa la Oficina Nacional de Estadística de la Contraloría General de la República, es así como se crea la Dirección Nacional de Estadística, dependencia directa de la Presidencia de la República. En el mes de octubre de 1953 bajo el gobierno del General Gustavo Rojas Pinilla, con amparo en el Decreto 2666, se crea el Departamento Administrativo Nacional de Estadística – DANE; posteriormente fue reorganizado en 1968 (Decreto 3167), siendo Presidente Carlos Lleras Restrepo; en diciembre de 1992, durante el gobierno de César Gaviria Trujillo, se llevó a cabo una reestructuración con base en el Decreto 2118. Mediante Decreto No.1174 del 29 de junio de 1999, bajo el gobierno de Andrés Pastrana, se adscribe al DANE el Instituto Geográfico Agustín Codazzi. Con el Decreto 1151 del 19 de junio de 2000, se adoptó una nueva estructura orgánica y posteriormente se realizaron los ajustes y modificaciones a la planta de personal, la cual fue adoptada mediante el Decreto 1187 del 28 de junio de 2000, en el gobierno de Andrés Pastrana Arango. Con el Decreto 263 del 28 de enero de 2004 se modifica la planta de personal del Departamento Administrativo Nacional de Estadística y se dictan otras disposiciones. Con el Decreto 262 del 28 de enero de 2004 se modifica la estructura del Departamento Administrativo Nacional de Estadística DANE y se dictan otras disposiciones.

Misión. Producir y difundir información estadística de calidad para la toma de decisiones y la investigación en Colombia, así como desarrollar el Sistema Estadístico Nacional.

Visión. En el 2018 el DANE se consolidará como una institución moderna, innovadora y generadora de conocimiento y continuará siendo la entidad líder en la producción estadística.

Propósito superior. Contribuimos al desarrollo del país produciendo y difundiendo información confiable, relevante, oportuna y de calidad.

Objetivos. El Departamento Administrativo Nacional de Estadística, DANE, tiene como objetivos garantizar la producción, disponibilidad y calidad de la información estadística estratégica, y dirigir, planear, ejecutar, coordinar, regular y evaluar la producción y difusión de información oficial básica. (Decreto 262 de 2004. Cap.1º/ Art.1º)

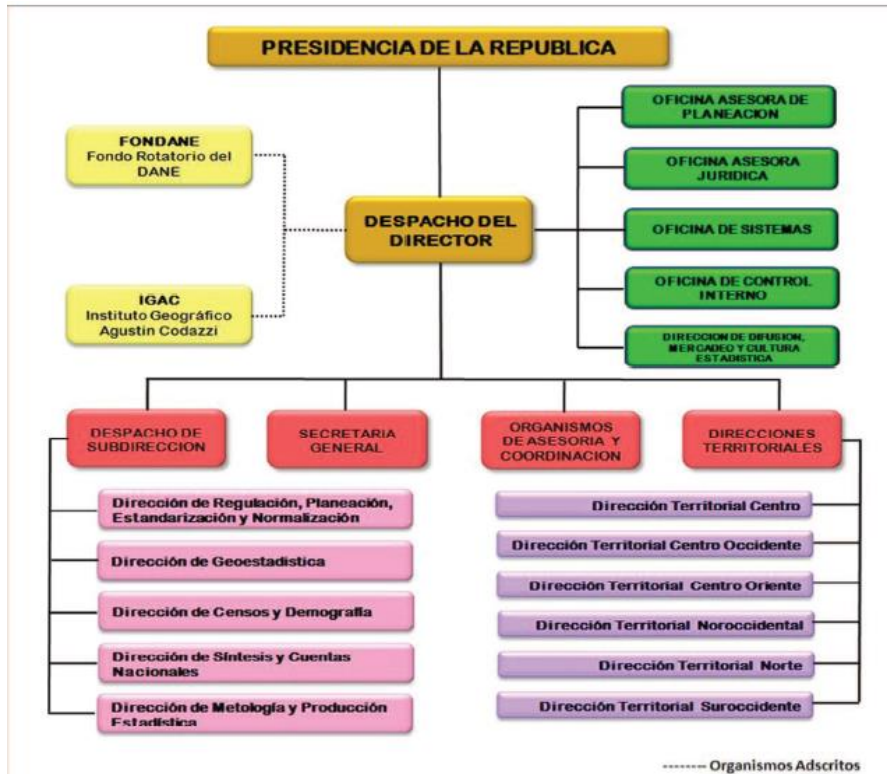
Objetivos estratégicos

1. Orientar el proceso de planeación de la Entidad a resultados integrales, que permita articular lo estratégico, táctico y operativo.
2. Aumentar la productividad y articulación del talento humano para que responda a las necesidades del DANE.

3. Regular, dirigir y coordinar el Sistema Estadístico Nacional mediante la formulación, ejecución, seguimiento, evaluación y divulgación del Plan Estadístico Nacional y los Planes Estadísticos Sectoriales y Territoriales y el aseguramiento de la calidad de las operaciones estadísticas; asesorar a los productores de estadísticas en el mejoramiento de los registros administrativos y la producción estadística.
4. Mejorar el nivel de desagregación territorial y regional en la información.
5. Estadística, de acuerdo a las necesidades y prioridades del país.
6. Dirigir, programar, ejecutar, coordinar, regular y evaluar la producción y difusión de las estadísticas oficiales que requiera el país y su georreferenciación según el caso.
7. Elaborar las cuentas nacionales anuales, trimestrales, regionales y satélites, para evaluar el crecimiento económico.
8. Fomentar la cultura estadística, promoviendo el desarrollo de la información estadística, su divulgación y utilización a nivel nacional, sectorial y territorial.
9. Facilitar el acceso y uso oportuno de los productos y servicios estadísticos a nivel nacional e internacional, en apoyo a los procesos de planificación y desarrollo integral del país y su articulación al contexto global.
10. Adoptar tecnologías de información y comunicaciones, que respondan a las necesidades de la entidad y del Sistema Estadístico Nacional.
11. Mantener y actualizar el Sistema de Información Geoestadístico como herramienta de gestión de información y fortalecimiento del Marco Geoestadístico Nacional para apoyar los procesos estadísticos, como componente del Sistema Estadístico Nacional.
12. Revisar, mejorar y difundir en forma permanente los marcos teóricos, metodológicos y operativos de las investigaciones estadísticas de acuerdo a los estándares internacionales y los requerimientos de la OCDE.
13. Mejorar, mantener y articular los sistemas de control interno y de gestión de calidad del DANE a través de un sistema integrado de gestión.
14. Fortalecer la cultura de administración de los riesgos del DANE para su identificación, prevención y mitigación permanente.
15. Divulgar los metadatos y resultados de las investigaciones estadísticas, en lenguaje sencillo y diferenciado para cada tipo de usuario de la información estadística.

2.3.2 Estructura organizacional.

Figura 5. Organigrama



Fuente: DANE

Funciones general. Según el Artículo 2 del Decreto 262 del 28 de enero de 2004, el Departamento Administrativo Nacional de Estadística tendrá, además de las funciones que determina el artículo 59 de la Ley 489 de 1998, las siguientes:

Relativas a la producción de estadísticas estratégicas:

- Diseñar, planificar, dirigir y ejecutar las operaciones estadísticas que requiera el país para la planeación y toma de decisiones por parte del Gobierno Nacional y de los entes territoriales.
- Realizar, directamente o a través de terceros, las actividades de diseño, recolección, procesamiento y publicación de los resultados de las operaciones estadísticas.
- Definir y producir la información estadística estratégica que deba generarse a nivel nacional, sectorial y territorial, para apoyar la planeación y toma de decisiones por parte de las entidades estatales.
- Producir la información estadística estratégica y desarrollar o aprobar las metodologías para su elaboración.

- Velar por la veracidad, imparcialidad y oportunidad de la información estadística estratégica.
- Dictar las normas técnicas relativas al diseño, producción, procesamiento, análisis, uso y divulgación de la información estadística estratégica.
- Elaborar el Plan Estadístico Nacional y someterlo a la aprobación del CONPES, por intermedio del Departamento Nacional de Planeación, y promover su divulgación.
- Coordinar y asesorar la ejecución del Plan Estadístico Nacional y de los planes estadísticos sectoriales y territoriales, hacer su seguimiento, evaluación y divulgación.
- Certificar la información estadística, siempre que se refiera a resultados generados, validados y aprobados por el Departamento.
- Diseñar y desarrollar el Sistema de Información Geoestadístico y asegurar la actualización y mantenimiento del Marco Geoestadístico Nacional.
- Generar y certificar las proyecciones oficiales de población de las entidades territoriales del país.
- Solicitar y obtener de las personas naturales o jurídicas, domiciliadas o domiciliadas en Colombia, y de los nacionales con domicilio o residencia en el exterior, los datos que sean requeridos para dotar de información estadística al país.
- Imponer multas como sanción a las personas naturales o jurídicas que incumplan lo dispuesto en la Ley 79 de 1993, previa investigación administrativa.
- Ordenar, administrar, adaptar y promover el uso de las clasificaciones y nomenclaturas internacionales en el país, para la producción de la información oficial básica.
- Las demás que le sean asignadas por la ley y por el reglamento.

Relativas a la Síntesis de Cuentas Nacionales:

- Elaborar las cuentas anuales, trimestrales, nacionales, regionales y satélites, para evaluar el crecimiento económico nacional, departamental y sectorial.
- Elaborar y adaptar a las condiciones y características del país, las metodologías de síntesis y cuentas nacionales, siguiendo las recomendaciones internacionales.
- Promover la divulgación y capacitación del sistema de síntesis y cuentas nacionales, tanto para productores como para usuarios de estadísticas macroeconómicas
- Las demás que le sean asignadas por la ley y por el reglamento.

Relativas a la producción y difusión de información oficial básica:

- Dirigir, programar, ejecutar, coordinar, regular y evaluar la producción y difusión de información oficial básica.
- Establecer las estrategias, los instrumentos y los mecanismos necesarios para elaborar y coordinar el Plan Nacional de Información Oficial Básica.
- Establecer y aprobar las normas técnicas y las metodologías convenientes para la producción y divulgación de la información oficial básica del país.

- Oficializar, adoptar y adaptar las nomenclaturas y clasificaciones usadas en el país para la producción y uso de la información oficial básica, así como asesorar sobre la implementación y uso de las mismas.
- Promover la adopción y adaptación de estándares de producción de información geográfica y espacial, que garanticen la georeferenciación de la información oficial básica.
- Impulsar la implementación de sistemas de información oficial básica a nivel regional y territorial.
- Diseñar las metodologías de estratificación y los sistemas de seguimiento y evaluación de dichas metodologías, para ser utilizados por las entidades nacionales y territoriales.
- Las demás que le sean asignadas por la ley y por el reglamento.

Relativas a la Difusión y Cultura Estadística:

- Difundir los resultados de las investigaciones que haga el Departamento en cumplimiento de sus funciones, de acuerdo con las normas de la reserva estadística.
- Fomentar la cultura estadística, promoviendo el desarrollo de la información estadística, su divulgación y su utilización a nivel nacional, sectorial y territorial.
- Las demás que le sean asignadas por la ley y por el reglamento.

2.3.3 Ficha institucional

Razón social: Departamento Administrativo Nacional de Estadística

Sector: Público Dirección:

Sede principal: Carrera 59 No. 26-70 Interior I – CAN

Ciudad: Bogotá D.C. – Colombia

Departamento: Cundinamarca

Territorial: Centro Oriente

Subsede: Cúcuta

Dirección: Calle 13 No. 5-09 Centro

Ciudad: Cúcuta

Departamento: Norte de Santander

2.3.4 Descripción de las Investigaciones Continuas del DANE en la Subsede de Cúcuta

GRAN ENCUESTA INTEGRADA DE HOGARES – GEIH

La Gran Encuesta Integrada de Hogares es la encuesta especializada en la medición de la estructura del mercado laboral y los ingresos de los hogares. Esta encuesta solicita información sobre las condiciones de empleo de las personas (si trabajan, en qué trabajan, cuánto ganan, si tienen seguridad social en salud o si están buscando empleo), fuentes de ingresos, así como características generales de la población como sexo, edad, estado civil y nivel educativo. Tiene una muestra total anual de 240.000 hogares aproximadamente.

El Objetivo de esta encuesta es Proporcionar información básica sobre el tamaño y estructura de la fuerza de trabajo (empleo, desempleo e inactividad) de la población del país, así como de las características sociodemográficas de la población colombiana.

La Gran Encuesta Integrada de Hogares Permite:

- Clasificar la población de cada uno de los dominios de estudio, según los conceptos y definiciones de la fuerza de trabajo establecidos por la Conferencia Internacional de Estadísticos del Trabajo (CIET) de la Oficina de la Organización Internacional de Trabajo (OIT) de 1983.
- Calcular los principales indicadores del mercado laboral: Tasa Global de participación (TGP), Tasa de Ocupación (TO), Tasa de desempleo (TD), Tasa de subempleo (TS) y su variación en el tiempo.
- Medir características generales de la población, vivienda, acceso a servicios públicos, sistema de protección social.
- Obtener información sobre variables sociodemográficas de la población, como: sexo, edad, estado civil, educación, etc.
- Medir las características del empleo: temporalidad, subempleo, rama de actividad, ocupación u oficio, posición ocupacional, ingreso, afiliación a la seguridad social, etc.
- Medir las características del desempleo: tiempo de búsqueda de empleo, rama de actividad, ocupación u oficio que desempeño en su empleo anterior.
- Medir las características de la inactividad y las razones por las que la población se ha retirado o no participa en el mercado laboral.
- Proporcionar información básica sobre el tamaño y la estructura de la población ocupada en empresas de hasta cinco trabajadores, así como las características sociodemográficas de esta población.
- Conocer los ingresos de los hogares tanto en dinero como en especie, que sirvan de insumo para las mediciones sobre pobreza.
- Proporcionar información sobre calidad del empleo

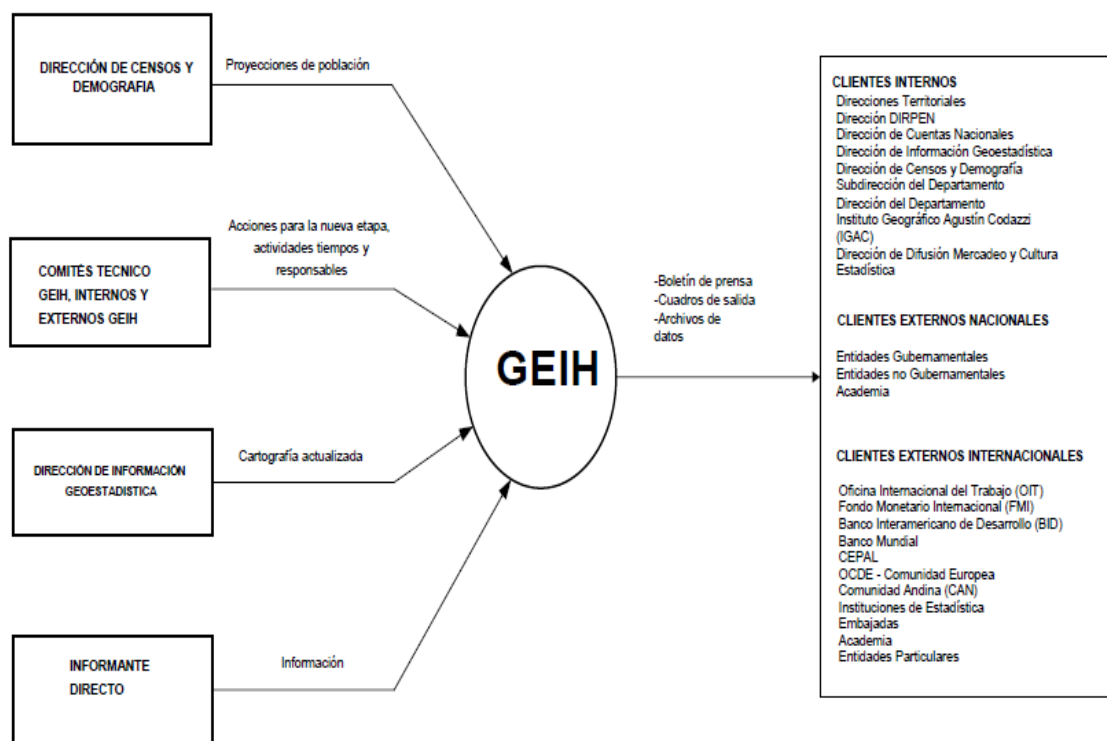
Adicionalmente, los principales indicadores que se obtienen a través de la Gran Encuesta Integrada de Hogares son los siguientes:

- TASA DE DESEMPLEO. $TD = (DS / PEA) * 100$. Es la relación porcentual entre el número de personas que están buscando trabajo (DS), y el número de personas que integran la fuerza laboral, la cual está constituida por la población económicamente activa (PEA).

- TASA GLOBAL DE PARTICIPACIÓN. $TGP = (PEA/PET) * 100$. Es la relación porcentual entre la población económicamente activa (PEA) y la población en edad de trabajar (PET). Este indicador refleja la presión de la población en edad de trabajar sobre el mercado laboral.

- TASA BRUTA DE PARTICIPACIÓN. $TBP = (PEA / PT) * 100$. Este indicador muestra la relación porcentual entre el número de personas que componen el mercado laboral (PEA), frente al número de personas que integran la población total (PT).
- TASA DE SUBEMPLEO. $TS = (PS / PEA) * 100$. Es la relación porcentual de la población subempleada (PS) y el número de personas que integran la fuerza laboral (PEA).
- TASA DE OCUPACIÓN. $TO = (OC/PET) * 100$. Es la relación porcentual entre la población ocupada (OC) y el número de personas que integran la población en edad de trabajar (PET).
- PORCENTAJE DE POBLACIÓN EN EDAD DE TRABAJAR (PET). $\% PET = (PET/PT)$. Este indicador muestra la relación porcentual entre el número de personas que componen la población en edad de trabajar (PET), frente a la población total (PT).

Figura 6. Diagrama de Contexto GEIH



Fuente: DANE

CENSO DE EDIFICACIONES – CEED

Entre las Estadística que el DANE desarrolla se encuentran las construcción, cuyo comportamiento hasta el año 1996, se venía calculando exclusivamente con los indicadores de licencias de construcción, del Índice de Costos de la Construcción de Vivienda y del

consumo aparente de cemento. A partir de 1996 la entidad diseña e implementa con el Censo de Edificaciones, procedimientos operativos para la realización de estudios que proporcionan información trimestral sobre la evolución, producción y comportamiento de las actividades de edificación.

La cobertura y desagregación geográfica de la recolección de información está conformada por las siguientes Áreas Urbanas (AU) y Áreas Metropolitanas (AM):

Desde Abril de 1997

- AU de Bogotá D.C., Soacha
- AM Medellín, Bello, Itagüí, Envigado, Barbosa
- AU Cali, Yumbo
- AU Barranquilla, Soledad
- AM Bucaramanga, Floridablanca, Girón, Piedecuesta
- AU Pereira, Dosquebradas
- AU Armenia

Desde Enero de 2000

- Armenia AU

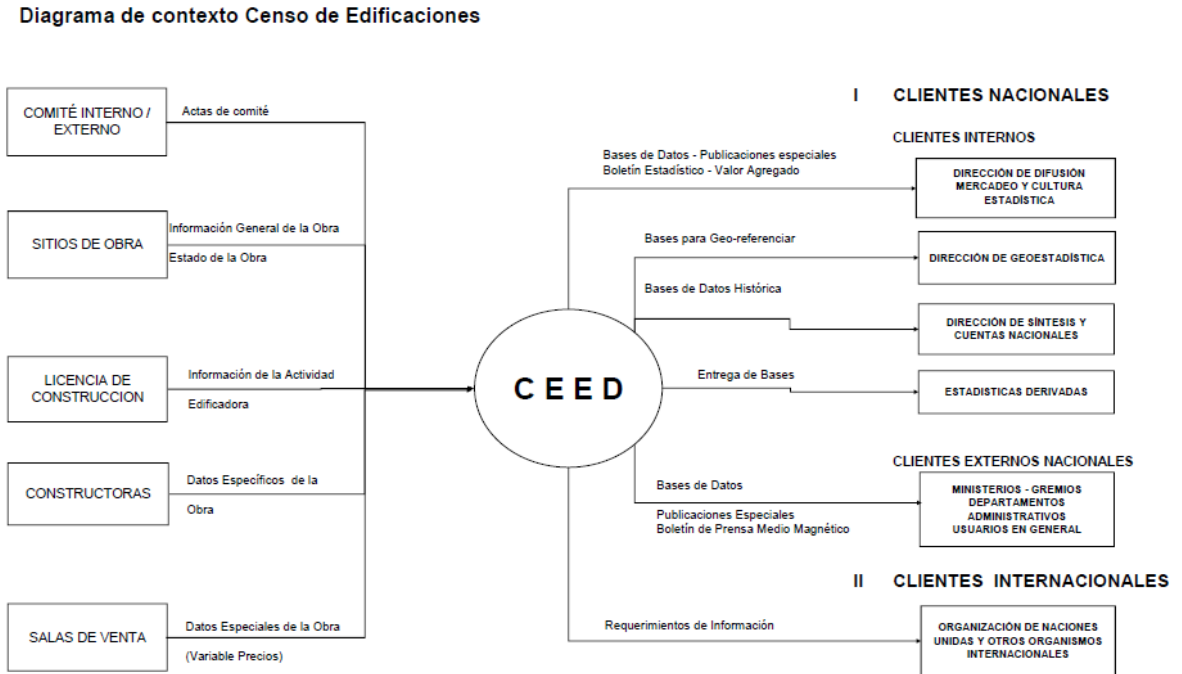
Desde Enero de 2002

- Sabaneta, Estrella, Caldas Copacabana, Girardota,

Desde julio de 2007

- AM Cúcuta, Los Patios, Villa del Rosario y el Zulia
- AU Manizales y Villa María
- AU Cartagena
- AU Villavicencio
- AU Pasto
- AU Popayán
- AU Ibagué
- AU Neiva

Figura 7. Diagrama de Contexto CEED



Fuente: DANE

ENCUESTA NACIONAL AGROPECUARIA – ENA

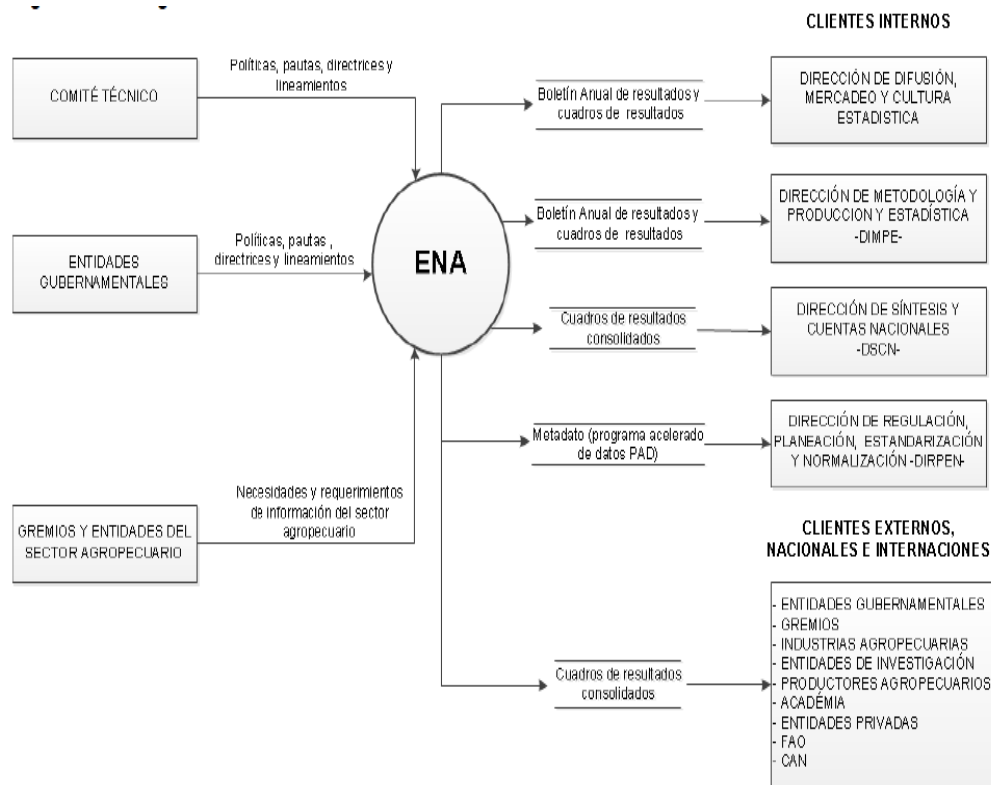
Tiene como objetivo. Estimar el uso de la tierra, el área, la producción y el rendimiento de los principales cultivos transitorios, permanentes, árboles frutales dispersos, el área en pastos y forestal, la producción de leche, especies menores y el inventario pecuario en 22 departamentos del territorio colombiano.

La Encuesta Producción Agrícola- ENA, provee cifras sobre área, producción y rendimiento de algunos cultivos transitorios y permanentes, los cuales pueden orientar la toma de decisiones por parte de los organismos encargados de la planificación del sector y de los inversionistas en el mismo.

Así como dar a conocer la caracterización sobre aspectos del sistema de comercialización de algunos cultivos transitorios y permanentes permitiendo obtener información sobre destinos, precios y sitios de venta.

A nivel Pecuario cuantificar las especies pecuarias por edad y sexo en las fincas con actividad pecuaria el día de la entrevista. Identificando principalmente las explotaciones con ganado vacuno de acuerdo con la orientación del hato, manejo y producción de leche.

Figura 8. Diagrama de Contexto ENA



Fuente: DANE

La ENA interactúa con otros sistemas a nivel interno y externo del DANE, en el ámbito externo las principales fuentes que proveen insumos e información son:

- Comité técnico: Políticas, pautas, directrices y lineamientos
- Entidades gubernamentales: Políticas, pautas, directrices y lineamientos
- Gremios y entidades del sector agropecuario: Necesidades y requerimientos de información del sector agropecuario.

La información que se genera una vez realizada la ENA se relaciona a continuación:

- Boletín de resultados anual
- Cuadros de salida

Esta información es suministrada a clientes internos y clientes externos nacionales e internacionales.

Clientes internos

- Dirección de difusión, mercadeo y cultura estadística
- Dirección de metodología y producción estadística DIMPE

- Dirección de síntesis y cuentas nacionales DSCN
- Dirección de regulación, planeación, estandarización y normalización DIRPEN

Clientes externos nacionales

- Entidades gubernamentales
- Gremios
- Industrias agropecuarias
- Entidades de investigación
- Productores agropecuarios
- Academia
- Entidades privadas

Clientes externos internacionales

- Organización de las naciones unidas para la agricultura y la alimentación –FAO-
- Comunidad andina – CAN-

A continuación se relacionan algunos de los principales cuadros de salida de la investigación, teniendo en cuenta las principales variables de estudio.

- Identificación
- Uso del suelo
- Área sembrada y número de unidades productoras según cultivo
- Área cosechada, producción y rendimiento de los principales cultivos
- Comercialización de los principales cultivos
- Otras variables de estudio cultivos transitorios
- Áreas sembradas y no cosechadas de cultivos transitorios
- Áreas sembradas y a cosechar de cultivos transitorios
- Cultivos de Hortalizas-área sembrada y unidades productoras
- Cultivos de Hortalizas -área cosechada, producción y rendimiento
- Cultivos Permanentes- área sembrada y unidades productoras
- Cultivos permanentes-área cosechados, producción y rendimiento
- Comercialización de los principales cultivos
- Otras variables de estudio cultivos permanentes
- Cultivos de Pastos y Forrajes
- Bosques Plantados
- Frutales
- Frutales Dispersos
- Actividad Pecuaria
- Manejo de pastos

ESTADÍSTICAS VITALES - EEVV

El Departamento Administrativo Nacional de Estadística – DANE, como órgano rector líder en la producción y difusión de las estadísticas estratégicas, es responsable, a través de la operación estadística Vitales (EE-VV), de producir las estadísticas de nacimientos y defunciones del país, utilizando como fuente de información los certificados de nacido vivo y de defunción, diligenciados por el personal médico de las Instituciones Prestadoras de Salud (IPS), Instituto Nacional de Medicina Legal (INML-CF) y funcionarios de Registro Civil.

Los certificados son diligenciados en medio físico (papel) o en medio electrónico (vía web) mediante una plataforma electrónica perteneciente al Sistema Integral de Información de la Protección Social (SISPRO) del Ministerio de Salud y Protección Social (MSPS), a través del módulo de nacimientos y defunciones del Registro Único de Afiliados (RUAF-ND). Comités interinstitucionales y Organismos internacionales que dan lineamientos y recomendaciones para el buen funcionamiento de las EEVV, son:

- Comisión Intersectorial de Gestión de las EEVV.
- Comités de EEVV Territoriales.
- Organismos Internacionales.

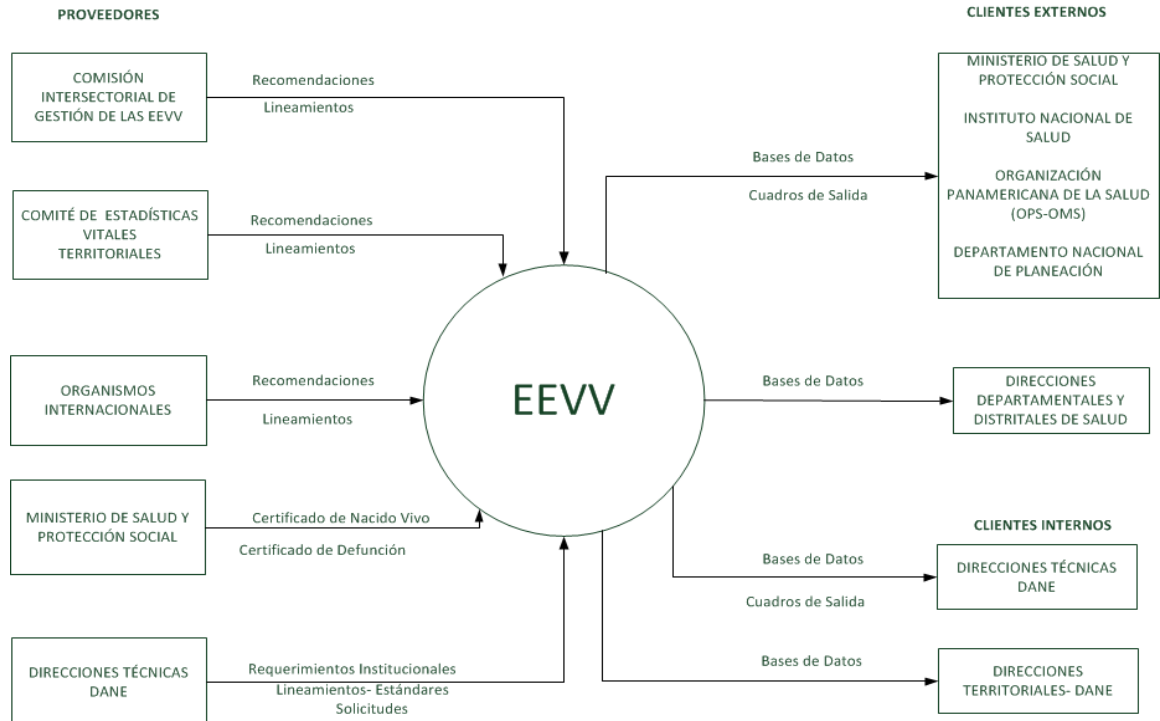
Fuentes generadoras de información de nacimientos y defunciones:

- Instituciones Prestadoras de Salud
- Instituto Nacional de Medicina Legal y Ciencias Forenses INML-CF
- Oficinas de Registro Civil (Notarías y Registradurías municipales)
- Direcciones Departamentales y Distritales de Salud.

Clientes internos y externos de la información:

- Ministerio de Salud y Protección Social
- Departamento Nacional de Planeación -DNP
- Instituto Nacional de Salud
- Direcciones Departamentales y Distritales de Salud

Figura 9. Diagrama de Contexto EEVV



Fuente: DANE

A partir de las bases de datos depuradas de nacimientos y de defunciones se generan los cuadros de salida, mediante la utilización de paquete de software estadístico. Una vez revisados se editan, se aprueban y se envían a la Dirección de Difusión, Mercadeo y Cultura Estadística, para ser publicados en la página web del DANE.

Los cuadros de Salida de Estadísticas Vitales, publicados en la página web de la entidad, nos dan a conocer datos referentes al número total de nacimientos en Colombia por área, sexo, según departamento y municipio de ocurrencia, departamento y municipio de residencia de la madre; esta información se constituye en fuente básica para el cálculo de indicadores como tasa bruta de natalidad, tasas de fecundidad y tasa de mortalidad infantil. A continuación se relacionan los cuadros de salida o resultados de la investigación estadísticas Vitales (EE-VV).

Cuadros de salidas de Nacidos Vivos

- Nacimientos por área de ocurrencia y sexo, según grupos de edad de la madre, total nacional
- Nacimientos por área y sexo, según departamento y municipio de ocurrencia
- Nacimientos por área y sexo, según departamento y municipio de residencia de la madre
- Nacimientos por tipo de parto según departamento de ocurrencia y sitio del parto

- Nacimientos por persona que atendió el parto según departamento, municipio de ocurrencia y sitio del parto
- Nacimiento por peso al nacer según departamento y área de residencia de la madre
- Nacimiento por peso al nacer según departamento, municipio y área de residencia de la madre
- Nacimientos por grupo de edad de la madre, según departamento y municipio de residencia de la madre
- Nacimientos por grupo de edad de la madre, según departamento de residencia de la madre
- Nacimiento por tiempo de gestación según departamento, municipio y área de residencia de la madre
- Nacimientos por número de hijos nacidos vivos, según departamento y municipio de residencia de la madre.
- Nacimientos por tipo de parto, según departamento de residencia de la madre y multiplicidad del embarazo
- Nacimientos por área y sexo, según departamento de residencia de la madre y pertinencia étnica del nacido vivo
- Nacimientos por sitio de parto, según departamento, municipio de ocurrencia y régimen de seguridad social de la madre

Cuadros de salidas de Defunciones Fetales

- Defunciones fetales por área y sexo, según departamento de ocurrencia -Total Nacional
- Defunciones fetales por área y sexo, según departamento y municipio de ocurrencia
- Defunciones fetales por sitio donde ocurrió la defunción y sexo, según departamento de ocurrencia.
- Defunciones fetales por grupos de edad de la madre, según departamento de residencia de la madre y grupos de causas de defunción (lista Colombia 105 para la tabulación de mortalidad)
- Defunciones fetales por tiempo de gestación, según departamento de residencia y grupo de edad de la madre
- Defunciones fetales por multiplicidad y muerte con relación al parto, según departamento de residencia y grupo de edad de la madre
- Defunciones fetales por sexo, según departamento, municipio de residencia de la madre y grupos de causas de defunción (lista de causas agrupadas 6/67 cie-10 de OPS)
- Defunciones fetales por tiempo de gestación, según departamento de residencia de la madre y grupos de causas de defunción (lista Colombia 105 para tabulación de la mortalidad)
- Defunciones fetales por número de hijos nacidos vivos, según departamento, municipio de residencia y grupo de edad de la madre
- Defunciones fetales por grupos de edad de la madre, según departamento de residencia y nivel educativo de la madre

- Defunciones fetales por peso al nacer, según departamento de residencia y grupo de edad de la madre.

Cuadros de salidas de Defunciones no Fetales

- Defunciones, por área donde ocurrió la defunción y sexo, según grupos de edad. Total nacional.
- Defunciones por persona que certifica la defunción, según departamento, área y sitio donde ocurrió la defunción.
- Defunciones por grupos de edad y sexo, según departamento, municipio y área donde ocurrió la defunción.
- Defunción por grupo de edad, sexo, según departamento, municipio y área de residencia.
- Defunciones por grupos de edad y sexo, según departamento, municipio de residencia y grupos de causas de defunción (lista de causas agrupadas 6/67 cie-10 de ops)
- Defunciones por sitio donde ocurrió la defunción, según departamento de ocurrencia y régimen de seguridad social
- Defunción por pertenencia étnica del fallecido y sexo, según departamento de residencia
- Defunción por probable manera de muerte y sexo, según departamento de ocurrencia
- Defunciones por grupo de edad y sexo, según departamentos de ocurrencia y grupos de causas de defunción (lista Colombia 105 para la tabulación de mortalidad)
- Defunciones por grupos de edad y sexo, según departamentos de residencia y grupos de causas de defunción (lista Colombia 105 para la tabulación de mortalidad)

Igualmente las bases de datos depuradas y los cuadros de salida son enviados a las siguientes entidades:

- Dirección de Difusión, Mercadeo y Cultura Estadística- DANE
- Direcciones Territoriales -DANE
- Ministerio de Salud y Protección Social- MSPS
- Organización Panamericana de la Salud -OMS/OPS
- Departamento Nacional de Planeación - DNP
- Instituto Nacional de Salud - INS
- Direcciones Departamentales y Distritales de Salud

SISTEMA DE INFORMACIÓN DE PRECIOS Y ABASTECIMIENTO DEL SECTOR AGROPECUARIO - SIPSA

Esta investigación se divide en tres componentes: Insumos, Precios mayoristas de alimentos y Abastecimientos.

El componente de insumos busca identificar los principales factores de producción y analizar el comportamiento del precio minorista de los insumos y factores asociados a la producción, útiles para el desarrollo de las actividades productivas agropecuarias. El objetivo principal es registrar y analizar los precios minoristas de insumos y factores asociados a la producción agropecuaria en el contexto nacional, a través de: I) registro y seguimiento del precio minorista de los insumos agrícolas y pecuarios con alta rotación (venta), II) registro y seguimiento del precio de otros factores asociados a la producción, III) análisis de factores y hechos que afectan el comportamiento de los precios de los factores mencionados, y IV) La recopilación, procesamiento y análisis de la información.

Precios Mayoristas tiene como objetivo suministrar información de precios de alimentos de consumo humano que se comercializan al por mayor en las centrales mayoristas y en los mercados regionales del país. Igualmente, se busca identificar las variables o factores que generan las variaciones en el mercado y analizar la dinámica de estos precios.

El componente de abastecimientos tiene como fin identificar la situación de abastecimiento de alimentos de las principales ciudades del país a través de agregados por ciudades y mercados obtenidos por medio del monitoreo al ingreso y salida de alimentos.

Esta encuesta tiene como metodología, la entrevista directa a comerciantes de las diferentes centrales de abasto y mercados mayoristas, comerciantes de insumos y factores de producción, de varios municipios incluidos en el Sistema, realizadas por encuestadores previamente capacitados.

La recolección de información se lleva a cabo en almacenes de comercialización minorista, centrales de abastos, peajes, ubicados en 140 municipios, y distribuidos en 21 departamentos. Además por su importancia, también se toman datos en tres mercados fronterizos: uno en la frontera con Ecuador y dos en la frontera con Venezuela.

ENCUESTA DE TRABAJO INFANTIL – ETI

Mediante convenios suscritos entre el DANE, el Ministerio de la Protección Social y el Instituto Colombiano de Bienestar Familiar ICBF y con el acompañamiento institucional del Departamento Nacional de Planeación DNP, realiza el seguimiento a los indicadores de trabajo infantil, con el fin de informar sobre las características demográficas de la población entre los 5 y los 17 años, su situación escolar, la magnitud del trabajo infantil y su participación en diferentes oficios en Colombia.

La Población Objetivo, corresponde a la población civil entre los 5 y los 17 años de edad, no institucional residente en todo el territorio nacional; excluyendo los nuevos

departamentos, denominados Territorios Nacionales antes de la constitución de 1991, en los cuales reside aproximadamente el 4% de la población.

Tiene cobertura nacional con resultados representativos para cabeceras y resto, así como para las veintitrés ciudades principales con sus áreas metropolitanas.

Periodos de Recolección:

Encuesta en profundidad cada 10 años. (2001 y 2011)

Módulo de seguimiento cada dos años 2003, 2005, 2007 y 2009.

Seguimiento anual a partir de 2012 (PND 2010-2014. Capítulo IV. Igualdad de oportunidades para la prosperidad social).

ENCUESTA AMBIENTAL DE INDUSTRIA - EAI

La Encuesta Ambiental Industrial es una encuesta económico – ambiental que tiene como objetivo obtener información de la inversión, costos y los gastos asociados a la protección del medio ambiente, la generación de residuos sólidos, el manejo del recurso hídrico y los instrumentos de gestión ambiental de la industria manufacturera.

Esta encuesta permite:

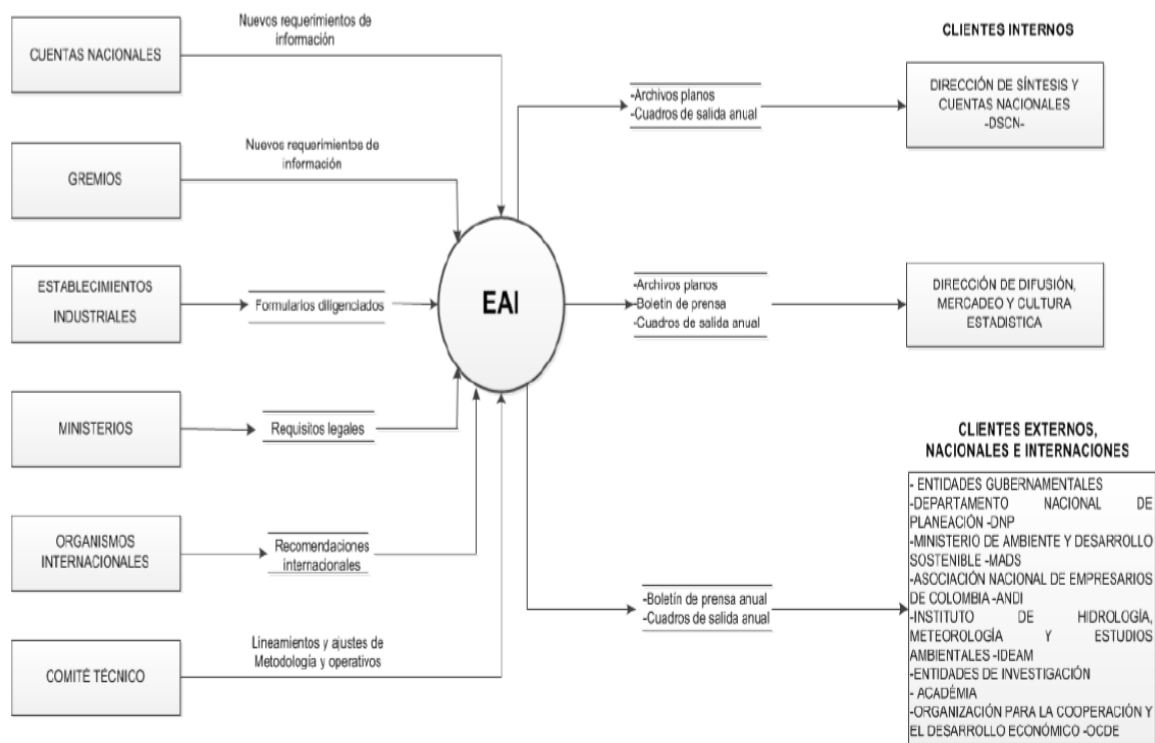
- Determinar el valor del gasto en protección ambiental de la industria manufacturera.
- Establecer la dinámica del manejo integrado de los residuos sólidos en los establecimientos industriales.
- Identificar el manejo y la gestión del recurso hídrico en los establecimientos industriales.
- Caracterizar la gestión ambiental realizada por la industria en sus establecimientos

Generar información ambiental estratégica sectorial que apoye la respuesta a los compromisos internacionales, relacionados con los protocolos suscritos por el país y los informes sobre el estado de los recursos naturales y el medio ambiente

La EAI tiene cobertura nacional. La población objetivo está conformada por aquellos establecimientos en el universo de estudio, que para el año 2010 reportaban información a la EAM (Encuesta Anual Manufacturera) junto a los nuevos establecimientos incluidos dentro del directorio 2010.

La Encuesta Ambiental de Industria – EAI, posee varias entradas, tanto internas como externas que proveen insumos y requerimientos para su desarrollo; entre estos se encuentran la Dirección de Síntesis y Cuentas Nacionales, los gremios, los ministerios y establecimientos industriales.

Figura 10. Diagrama de Contexto EAI



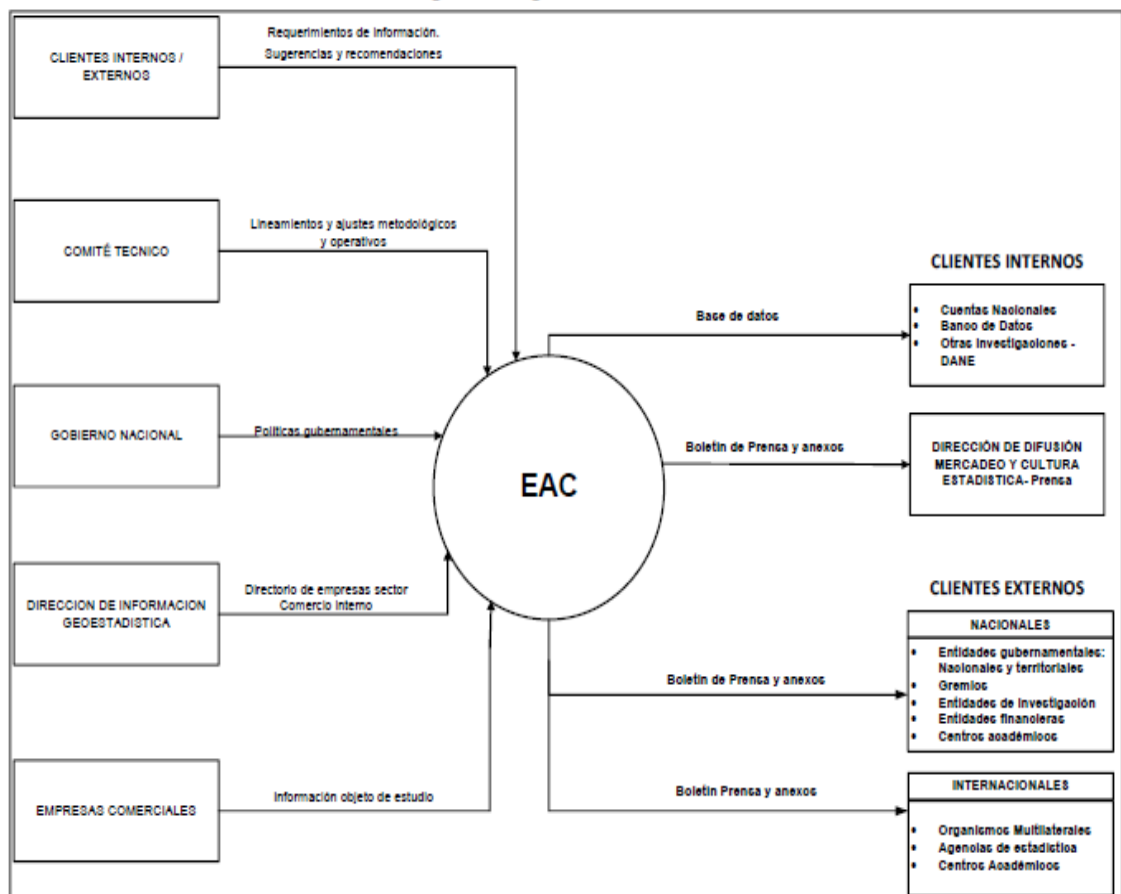
Fuente: DANE

ENCUESTA ANUAL DE COMERCIO – EAC

La Encuesta Anual de Comercio EAC, tiene como fin conocer la estructura y el comportamiento económico del sector comercio a nivel nacional, y por grupo de actividad comercial, de manera que permita el análisis de la evolución del sector y de la conformación de agregados económicos; determinando la estructura de cada una de las actividades económicas de comercio y permitiendo realizar análisis sectorial.

La Encuesta Anual de Comercio EAI, tiene cobertura nacional y la población objetivo, son las unidades económicas formalmente establecidas ubicadas en el territorio nacional dedicadas a las actividades de Comercio interior (al por mayor y al por menor).

Figura 11. Diagrama de Contexto ECA

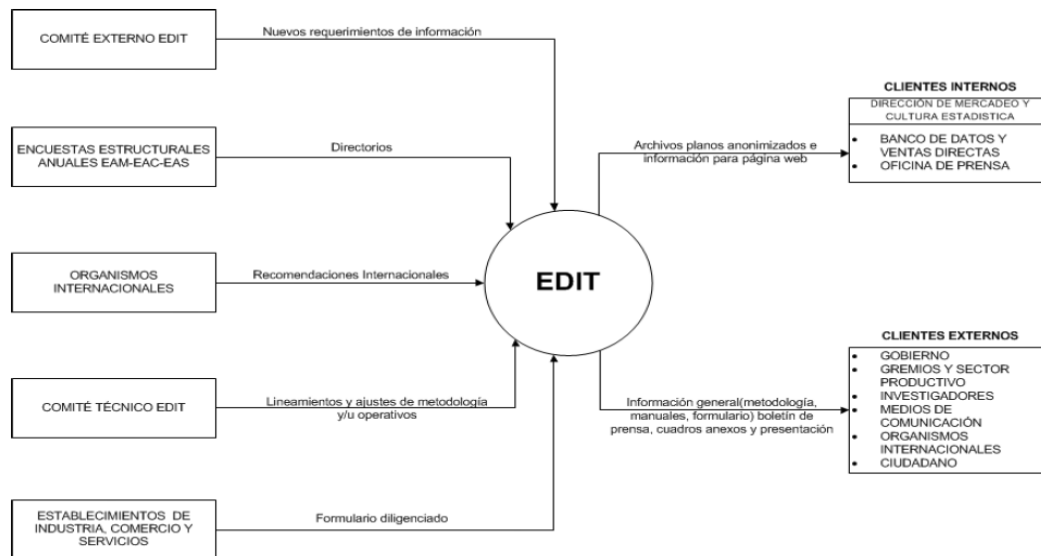


Fuente: DANE

ENCUESTA DE DESARROLLO E INNOVACIÓN TECNOLÓGICA - ETAPA INDUSTRIA

La Encuesta de Desarrollo e Innovación Tecnológica es la investigación económica por medio de la cual el Departamento Administrativo Nacional de Estadística - DANE obtiene la información del comportamiento de la innovación y desarrollo tecnológico, tanto en producto como actividades, en el sector industrial, servicios y comercio del país.

Figura 12. Diagrama de Contexto EDIT



Fuente: DANE

La Encuesta de Desarrollo e Innovación Tecnológica interactúa con varias fuentes, tanto a nivel interno como externo del DANE, las cuales proveen insumos y requerimientos indispensables para el desarrollo de la investigación, estas son:

- Comité externo de EDIT: aportan requerimientos de información de acuerdo con sus necesidades, como también sugerencias y recomendaciones de carácter metodológico.
- Encuestas estructurales anuales EAM-EAC-EAS: suministran el directorio actualizado de las empresas de los sectores industria, comercio interno y servicios.
- Organismos internacionales: aportan manuales e información de referencia a nivel internacional.
- Comité técnico EDIT: determina el diseño temático y operativo de la investigación, formula lineamientos, ajustes metodológicos y operativos.
- Establecimientos de industria, comercio y servicios: unidades económicas que proveen la información objeto de estudio de la investigación.

La información que se genera, una vez realizada la Encuesta de Desarrollo e Innovación Tecnológica, es la siguiente:

- Boletín de prensa
- Comunicado de prensa
- Anexos
- Cuadros de salida

Esta información es recibida por clientes tanto internos como externos:

Clientes internos:

Dirección de mercadeo y cultura estadística:

- Banco de datos y Ventas directas
- 2. Oficina de prensa

Clientes Externos:

- Gobierno
- Gremios y sector productivo
- Investigadores
- Medios de comunicación
- Organismos internacionales
- Ciudadano

MUESTRA MENSUAL MANUFACTURERA – MMM

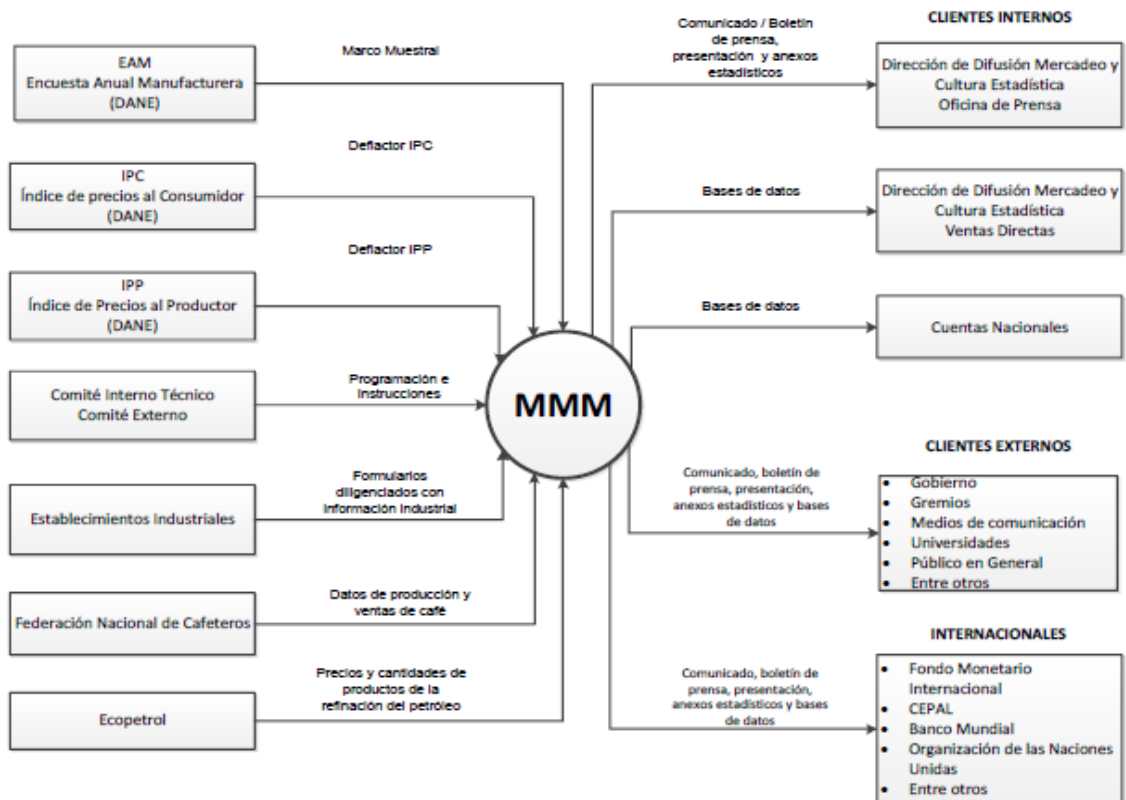
La información estadística sobre el sector manufacturero del país, se viene realizando de manera ininterrumpida desde mayo de 1962, a través de la muestra mensual de industria mediante la cual se obtiene la información básica necesaria para la generación de indicadores económicos que permiten medir en el corto plazo, la evolución de la industria nacional, a través de las variables de empleo, salarios, horas trabajadas, producción y ventas.

Esta encuesta le permite:

- Determinar el comportamiento y evolución mensual del sector manufacturero y de las diferentes actividades que lo conforman.
- Construir los indicadores sectoriales para el análisis de coyuntura económica.
- Construir el índice de producción real para la estimación provisional del Producto Interno Bruto – PIB.
- Servir de base para evaluaciones sectoriales por parte del sector gubernamental y privado.
- Construir el soporte básico para la elaboración de indicadores de competitividad (Productividad Laboral, re
- Remuneración por horas y costo laboral unitario).

El universo de estudio está constituido por la totalidad de los establecimientos que desarrollan actividades manufactureras en el territorio nacional. La Población Objetivo es el total de establecimientos industriales que según la Encuesta Anual Manufacturera, ocupaban 10 o más personas o que en su defecto presentaron niveles de producción anual iguales son superiores a \$ 130.5 millones de pesos de 2007.

Figura 13. Diagrama de Contexto MMM



Fuente: DANE

La Muestra Mensual Manufacturera interactúa con otras dependencias a nivel interno y externo del DANE. En el ámbito externo, se alimenta de tres fuentes principales que le proveen información sustantiva (Ver figura # 2), de la siguiente manera:

- Establecimientos Industriales: aportan la información industrial en los formularios electrónicos diligenciados.
- Federación Nacional de Cafeteros: suministra los datos de producción y venta de café.
- ECOPETROL: provee los precios y cantidades productos de la refinación del petróleo.

La Muestra se alimenta también de las siguientes dependencias internas:

- Encuesta Anual Manufacturera – EAM: que aporta el marco muestral.
- Índice de Precios al Consumidor – IPC: suministra el deflactor IPC
- Índice de Precios al Productor – IPP: suministra el deflactor IPP

La información que se genera una vez realizada la Muestra Mensual Manufacturera es la siguiente:

- Boletín MMM y sus anexos.

- Comunicado de prensa.
- Bases de datos.
- Presentación coyuntural.

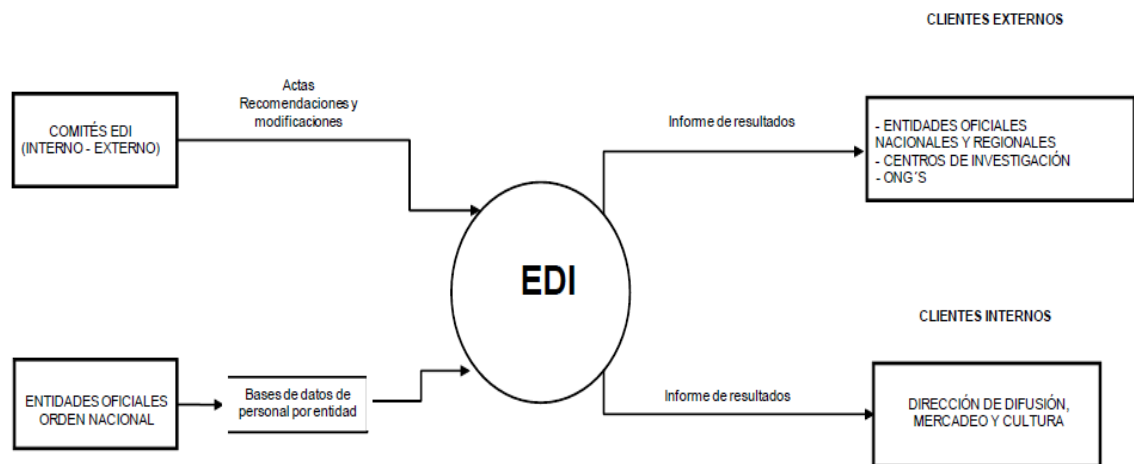
ENCUESTA SOBRE AMBIENTE Y DESEMPEÑO INSTITUCIONAL – EDI

La EDI, busca Obtener información sobre la percepción de los funcionarios respecto al ambiente institucional de las entidades, a partir del conocimiento sobre el nivel existente de credibilidad en las reglas, en las políticas y suficiencia de recursos y previsibilidad. Así como la percepción de desempeño institucional de las entidades, a través del conocimiento sobre los logros alcanzados en gestión por resultados, rendición de cuentas, bienestar laboral y prevención de prácticas irregulares. Para generar indicadores de desarrollo de la administración pública, que permitan clasificar las organizaciones en un momento dado y comparar su evolución a lo largo del tiempo.

La población objeto de estudio son los Servidores públicos con una antigüedad superior a seis meses en la entidad, y que laboran en la ciudad de Bogotá, de las entidades del nivel central de los poderes ejecutivo, legislativo y judicial, organismos de control y organización electoral.

Adicionalmente, los funcionarios que laboran en la sede principal de las Corporaciones autónomas regionales, universidades públicas, instituciones de investigación científica y ambiental ubicadas en el nivel regional. En total 162 entidades.

Figura 14. Diagrama de Contexto EDI



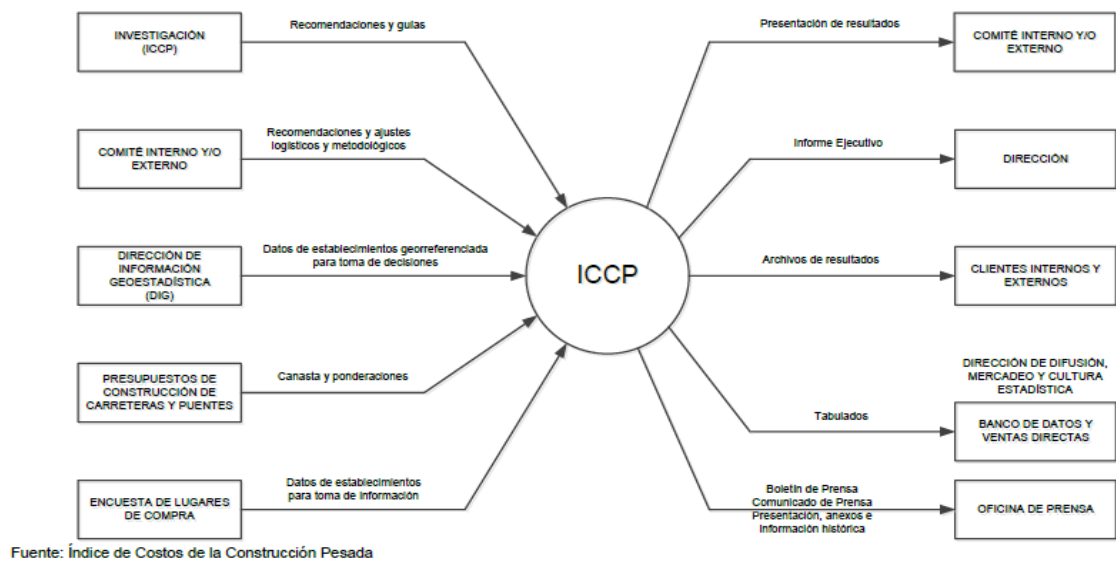
Fuente: DANE

ÍNDICE DE COSTOS DE LA CONSTRUCCIÓN PESADA – ICCP

Objetivo. Medir la variación porcentual promedio de los precios de una canasta de insumos representativos de la construcción de carreteras y puentes, indicando la proporción en que se aumentaron o disminuyeron los costos de los insumos en un período de estudio.

El universo de estudio son las constructoras encargadas de la construcción de carreteras y puentes en el territorio nacional. La población objetivo son los establecimientos económicos especializados en la venta y prestación de servicio de alquiler de equipos y suministro de salarios de mano de obra para la construcción de carreteras y puentes, en las ciudades de Armenia, Barranquilla, Bogotá, Bucaramanga, Cali, Cartagena, Cúcuta, Ibagué, Manizales, Medellín, Neiva, Pasto, Pereira, Popayán, Santa Marta y Villavicencio.

Figura 15. Diagrama de Contexto ICCP



Fuente: DANE

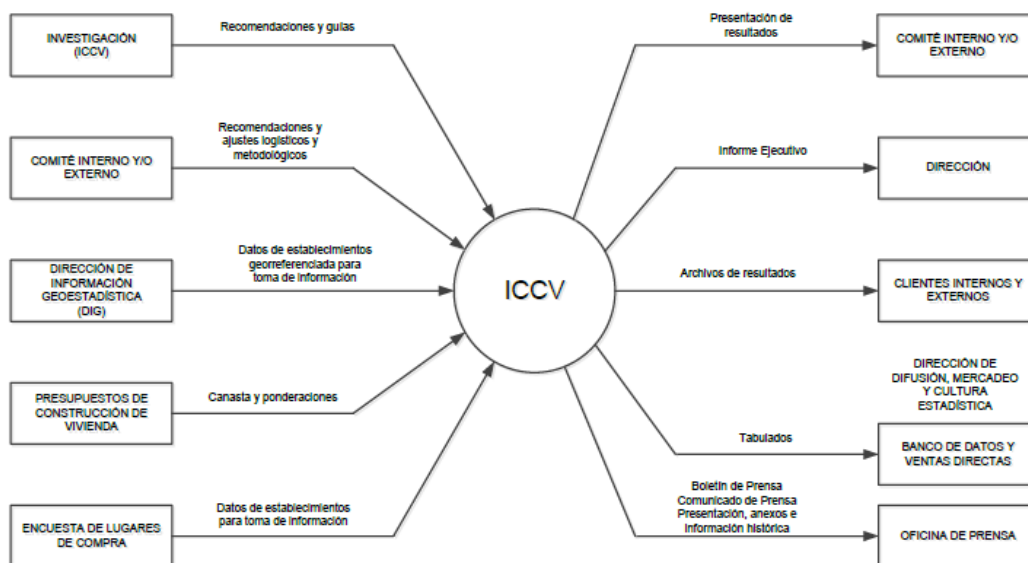
ÍNDICE DE COSTOS DE LA CONSTRUCCIÓN DE VIVIENDA – ICCV

En 1972, el DANE inicia la investigación sobre costos de la construcción de vivienda. El objetivo es proveer una medición de la variación mensual promedio, de los costos de un conjunto de insumos utilizados para la construcción de vivienda a nivel nacional, en quince ciudades investigadas por grupos de costos y tipos de vivienda.

El universo de estudio son las constructoras encargadas de la construcción de vivienda. La población objetivo son los establecimientos económicos especializados en la venta y prestación de servicio de alquiler de equipos y suministro de salarios de mano de obra para la construcción de vivienda, ubicados en las quince ciudades: Armenia, Barranquilla, Bogotá, Bucaramanga, Cali, Cartagena, Cúcuta, Ibagué, Manizales, Medellín, Neiva, Pasto,

Pereira, Santa Marta y Popayán. El alcance temático comprende la información sobre insumos y precios utilizados en la construcción de vivienda y se utiliza como método de recolección la entrevista directa con dispositivo móvil de captura DMC.

Figura 16. Diagrama de Contexto ICCV



Fuente: DANE

ÍNDICE DE COSTOS DE LA EDUCACIÓN SUPERIOR PRIVADA - ICESP

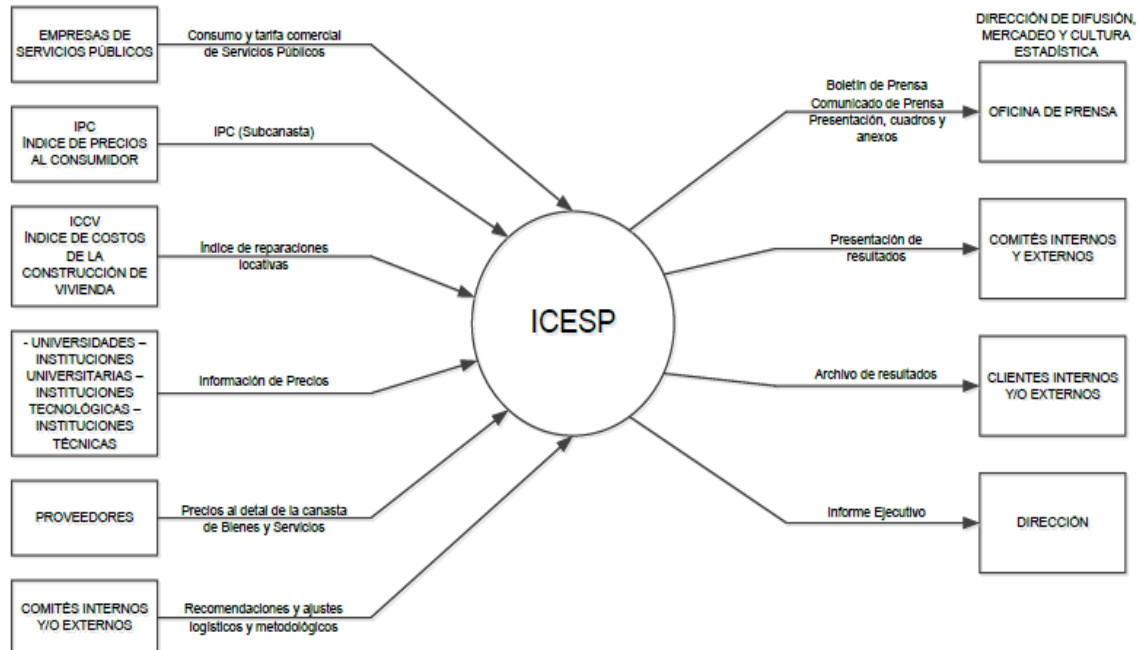
El ICESP es una investigación que permite calcular el promedio de las variaciones de precios de los bienes y servicios que adquieren las instituciones de educación superior privada, para el desarrollo de su actividad. El objetivo principal es establecer un indicador de la evolución semestral de los precios de los bienes y servicios que adquieren las instituciones de educación superior privada para el desarrollo de su objeto social.

El ICESP presenta resultados semestrales para el total nacional, generando índices por grupo, subgrupo y gastos básicos para los cuatro tipos de instituciones del sector privado: Universidades, Instituciones Universitarias, Instituciones tecnológicas e Instituciones técnicas. En esta investigación no se incluyen las instituciones del sector público, porque el alcance de la investigación delimitado por el convenio Ínter administrativo No 3226 de diciembre de 1995, solo incluía el desarrollo metodológico de un Índice de Costos de la Educación Superior Privada. (Las necesidades de información apuntaban a las instituciones de carácter privado exclusivamente).

La población objetivo son las instituciones de educación superior de carácter privado que están registradas ante el ICFES, y los establecimientos de la ciudad de Bogotá donde las instituciones adquieren los insumos que fueron establecidos dentro de la canasta del ICESP.

La información es recolectada en los meses de abril y mayo (primer semestre) y octubre y noviembre (segundo semestre), es representativa de la variación de precios observada para el semestre. El método de recolección es entrevista directa y auto diligenciamiento para las variables recolectadas en las instituciones de educación superior.

Figura 17. Diagrama de Contexto ICESP



Fuente: DANE

ÍNDICE DE PRECIOS AL CONSUMIDOR – IPC

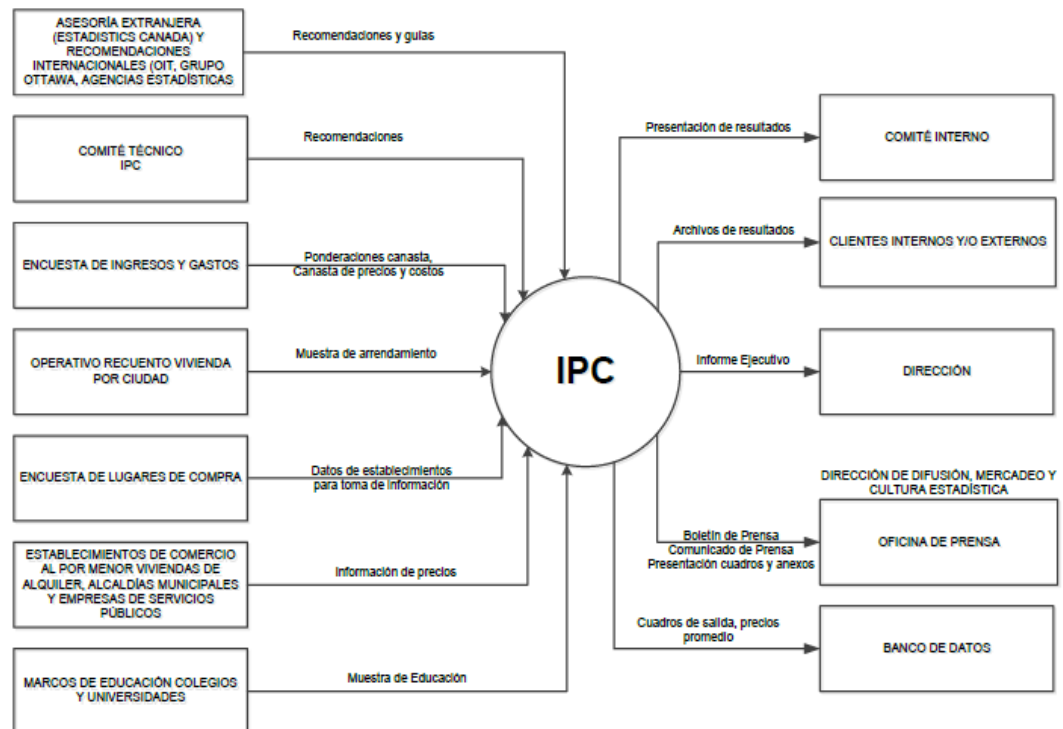
El objetivo de esta investigación es acumular y presentar, a partir de un mes base, la variación promedio mensual de una canasta de bienes y servicios representativa del consumo de los hogares del país.

El alcance temático es la información sobre artículos y precios enmarcados en el campo del consumo final de los hogares.

La población objetivo son todos los establecimientos en los cuales el consumidor adquiere bienes o servicios para ser consumidos, ubicados en las áreas urbanas de 24 capitales de departamentos.

El método de recolección es entrevista directa con el formulario único de recolección en medio físico o magnético.

Figura 18. Diagrama de Contexto IPC



Fuente: DANE

ÍNDICE DE PRECIOS AL PRODUCTOR – IPP

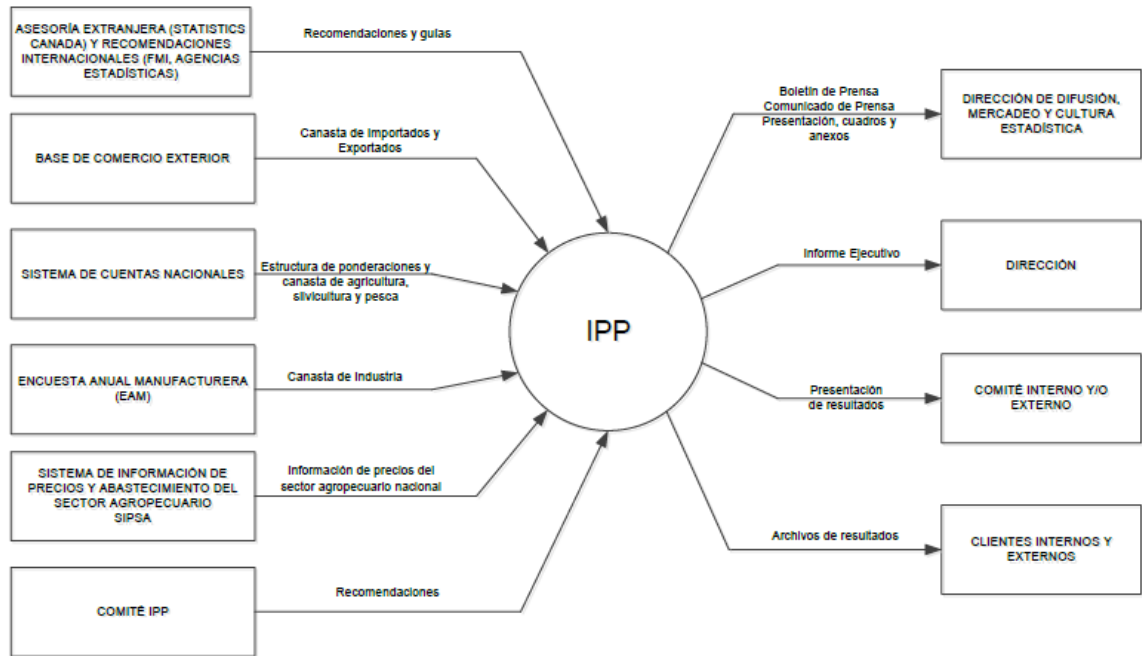
El cálculo del IPP se inició en el año 1990 en el Banco de la República. Este indicador tenía como propósito general, elaborar un conjunto de índices para medir los cambios en los precios en la primera etapa de comercialización de una canasta de bienes representativa de la oferta total de la economía.

El objetivo general es Proporcionar una medición de la variación mensual promedio de los precios de una canasta de bienes representativa de la oferta interna nacional en su primera etapa de comercialización. Esto incluye bienes producidos y vendidos por empresas tanto nacionales como importadoras.

El alcance temático comprende la información sobre precios de los artículos producidos y comercializados en el territorio nacional. La población objetivo está constituida por las empresas productoras y comercializadoras de bienes transportables.

El periodo de recolección esta entre el 15 y el 30 de cada mes. Para productos del sector agrícola, pecuario y pesca la recolección es semanal. El método de recolección so los medios electrónicos, auto diligenciamiento aplicativo web.

Figura 19. Diagrama de Contexto IPP



Fuente: DANE

ÍNDICE DE PRECIOS DE VIVIENDA NUEVA - IPVN

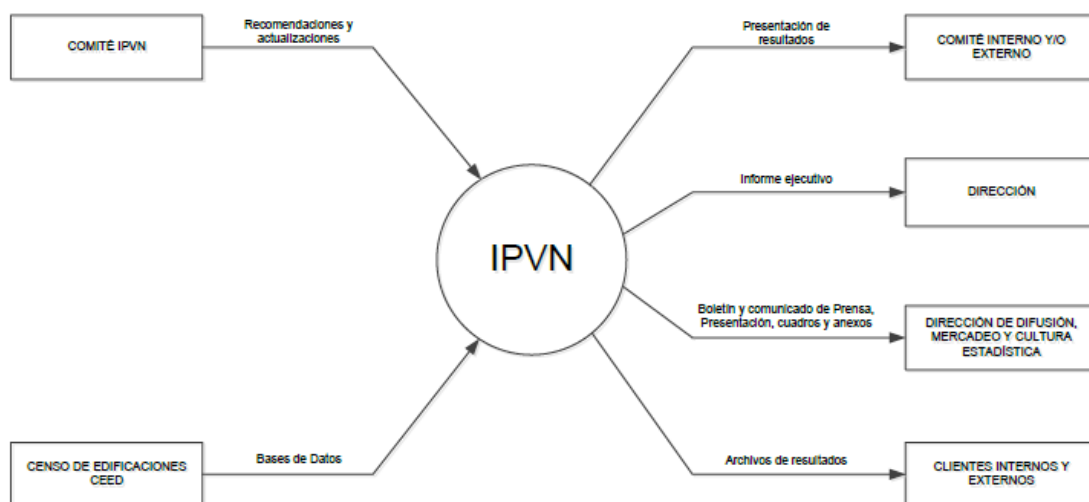
El DANE en su esfuerzo permanente por dotar al país con datos útiles y confiables, en el año 2000 construyó dos indicadores, los cuales permiten medir de manera directa la evolución de los precios de las viviendas (IPVN) y de las edificaciones que están en proceso de construcción (IPEN).

El objetivo principal IPVN es establecer la variación promedio trimestral de los precios de las viviendas nuevas en proceso de construcción y culminadas hasta la última unidad vendida a través de un índice de precios superlativo de Fisher.

El IPVN incluye dentro de su alcance, los precios de las obras (vivienda), destinadas a la venta, que son encontradas por primera vez en los operativos censales –CEED-; las obras en proceso de construcción y las culminadas hasta la última unidad vendida.

Se excluyen las obras que por algún fenómeno paralizan su proceso constructivo y las que continúan paralizadas al momento del realizar el operativo censal. Igualmente, son excluidas aquellas de uso propio, ya que los valores incorporados dentro del índice deben corresponder a precios de mercado.

Figura 20. Diagrama de Contexto IPVN



Fuente: DANE

ENCUESTA DE MICROESTABLECIMIENTOS - MICRO

La Encuesta de Microestablecimientos de comercio, servicio e industria, ha identificado la necesidad de contar con una documentación actualizada que describa los procedimientos que se realizan en la operación estadística.

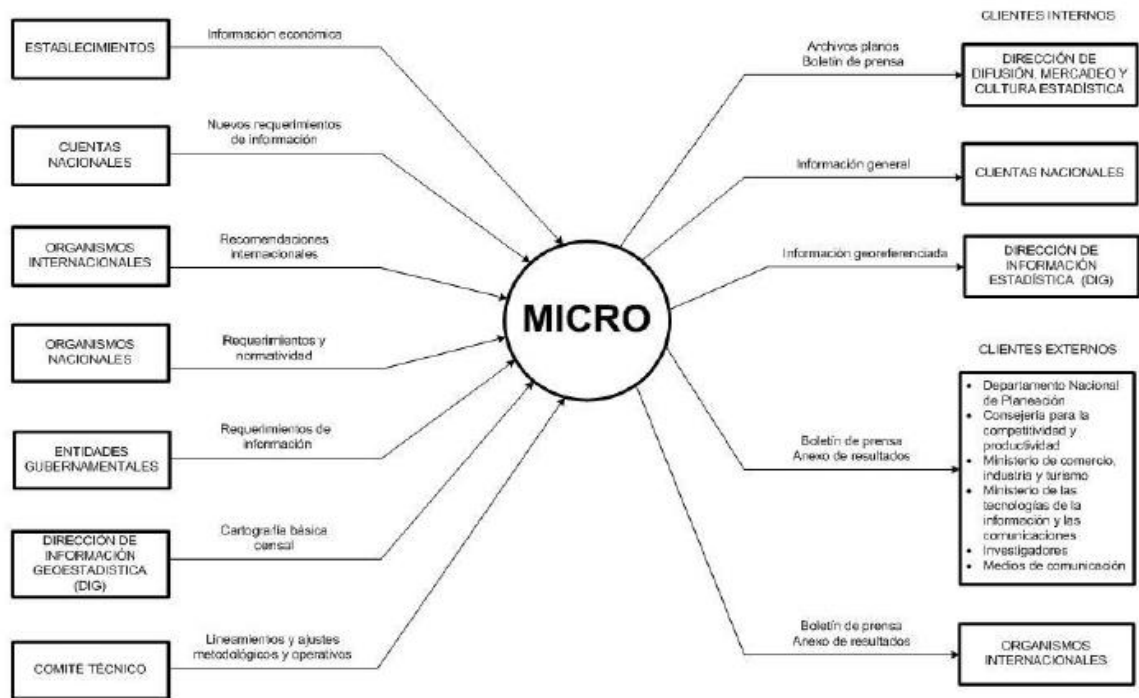
El objetivo es determinar la estructura en el mediano plazo (anual) de los microestablecimientos que cumplen con las siguientes características:

- Ocupan el mismo espacio físico
- Son identificados como la misma unidad lega (NIT, C.C, razón social o nombre comercial)
- Desarrollan actividades de industria, comercio o servicios y iv) llevan más de un año de operación, en las 24 ciudades principales y sus áreas metropolitanas con hasta nueve (9) personas ocupadas.

El alcance temático comprende los establecimientos con 9 o menos personas ocupadas de comercio al por mayor, el comercio al por menor y venta de motocicletas y sus accesorios, los talleres de mantenimiento y reparación de vehículos automotores. Todos los establecimientos de servicios sin incluir los financieros, la educación pública y los establecimientos del orden gubernamental. Toda la microindustria según la CIU Rev. 3 A.C.; que permanecieron en el mismo emplazamiento durante los años 2010 y 2011 y de los cuales se tiene información de su actividad económica.

El método de recolección de información es entrevista directa al propietario o administrador del establecimiento económico.

Figura 21. Diagrama de Contexto MICRO



Fuente: DANE

ENCUESTA ANUAL DE SERVICIOS - EAS

La Encuesta Anual de Servicios es una investigación económica que permite conocer la estructura y comportamiento económico del sector de los servicios en estudio en cuanto a su estructura, para la prestación del servicio, su desarrollo y evolución. También se obtiene información necesaria para la estimación de los valores absolutos de los principales agregados económicos, del sector.

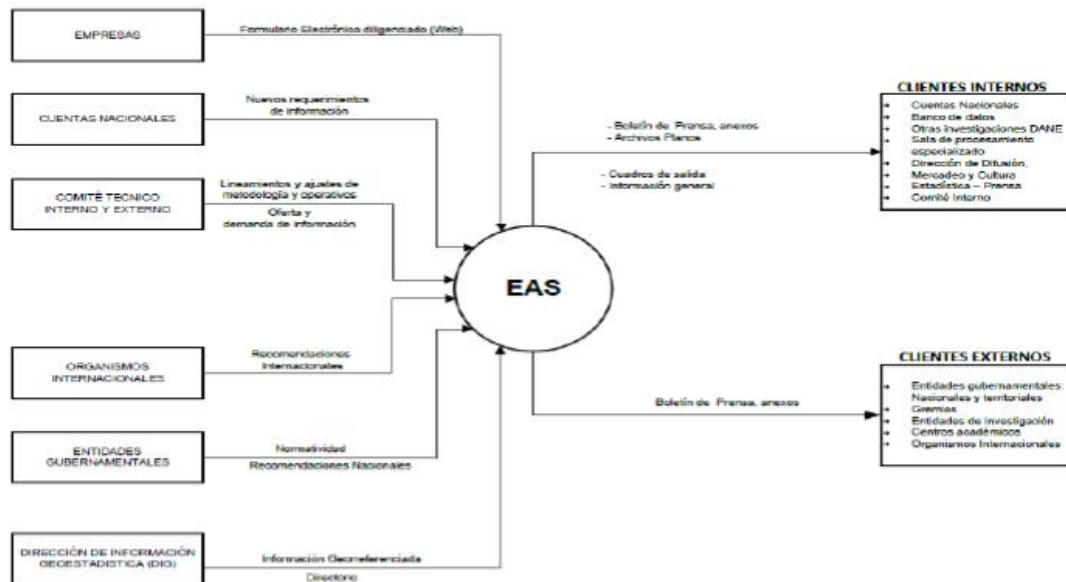
La investigación cubre las siguientes actividades de servicios determinadas en la CIU Rev. 3 adaptada para Colombia:

- Servicios de alojamiento en hoteles.
- Campamentos y otros tipos de hospedaje no permanente (grupo 551)
- Expendio de alimentos preparados en el sitio de venta y bebidas alcohólicas (grupos 552 y 553)
- Actividades complementarias y auxiliares al transporte (división 63 excepto clase 6340)
- Actividades de agencias de viajes (clase 6340)

- Actividades postales y de correo (grupo 641); telecomunicaciones (grupo 642)
- Actividades inmobiliarias, alquiler de maquinaria y equipo sin operario (divisiones 70 y 71)
- Informática y actividades conexas (división 72)

El universo de estudio está conformado por empresas formalmente establecidas, residentes en el territorio nacional, cuya principal actividad es la prestación de servicios, conforme a la delimitación establecida en el alcance temático.

Figura 22. Diagrama de Contexto EAS



Fuente: DANE

MUESTRA TRIMESTRAL DE SERVICIOS - MTS

La Muestra Trimestral de Servicios es una investigación económica que permite conocer el comportamiento económico y la evolución coyuntural del sector de los servicios a través de índices y variaciones para las variables de ingresos, personal ocupado y gastos de personal. El alcance temático, corresponde a las actividades económicas del sector servicios determinadas en la CIU Rev. 3 (Clasificación Industrial Internacional Uniforme. Revisión 3) adaptada para Colombia, descritos en la población objeto de estudio.

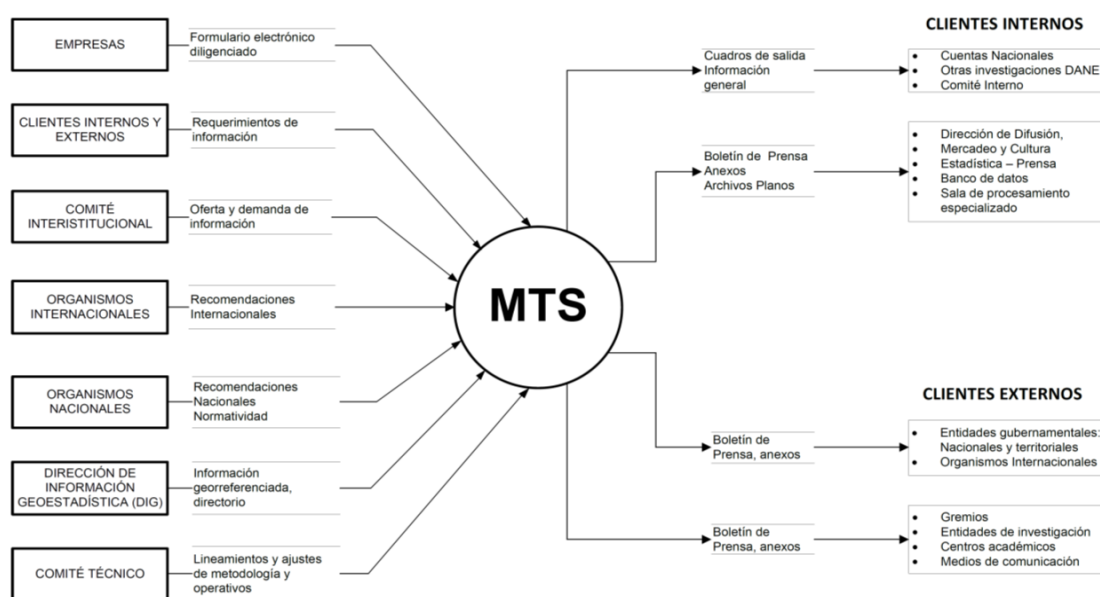
Exclusiones. Actividades de sindicatos, organizaciones religiosas, políticas, deportivas y otras actividades de esparcimiento, servicios del gobierno, gremios, organizaciones no gubernamentales, educación (excepto educación superior), transporte urbano de pasajeros. También se excluyen los puestos fijos, puestos móviles y viviendas con actividad económica.

Al considerar otras variables que logren captar la coyuntura del sector servicios, tal como indicadores de volumen y precios, se establece que comprende una mayor dificultad, tanto por su definición y heterogeneidad al interior de cada subsector, como por la baja disponibilidad de esta información en las empresas.

Las actividades investigadas corresponden a los servicios catalogados como de mercado, y se excluyen todas aquellas de no mercado.

El periodo se inicia el primer día hábil luego de la terminación del trimestre de referencia y se extiende hasta 60 días calendario.

Figura 23. Diagrama de Contexto MTS



Fuente: DANE

ENCUESTA DE CONVIVENCIA Y SEGURIDAD CIUDADANA - ECSC

Con el objetivo Generar información estadística sobre personas de 15 años y más, que han sufrido un perjuicio como consecuencia de acciones delictivas tales como hurto, riñas y peleas y/o extorsión. En 2011 el DANE, realizó en conjunto con el Ministerio de Defensa Nacional la prueba piloto de la Encuesta de Victimización en Cali, con el objetivo de probar el instrumento que permitiera obtener información estadística sobre personas de 15 años y más, que habían sufrido un perjuicio como consecuencia de acciones delictivas tales como hurto, violencia interpersonal o extorsión e indagar sobre la percepción de seguridad que tienen las personas. En abril de 2012 se repitió el ejercicio de la prueba piloto evaluando los cambios que fueron resultado del análisis de la primera piloto.

La ESCS contempla el hurto en sus tres modalidades (residencias, personas y vehículos); riñas y peleas, y extorsión. Así como la percepción frente a temas de convivencia ciudadana y confianza institucional.

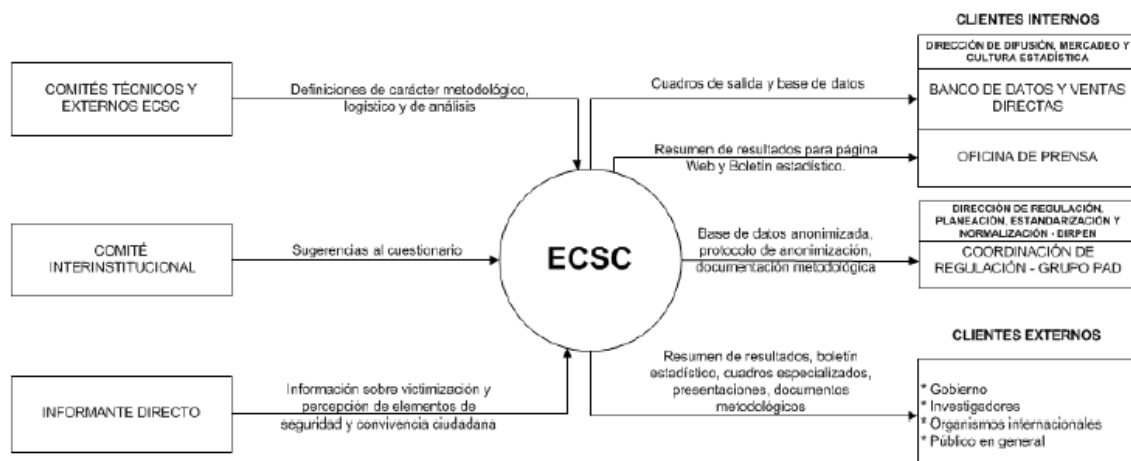
La información que se recoge en la encuesta tiene representatividad para personas de 15 años y más, en las 28 ciudades objeto de estudio. La encuesta no busca obtener información acerca de todos los delitos contenidos en el Código Penal colombiano ya que no son objeto de estudio de la encuesta.

La población objetivo está compuesta por los hogares particulares y población civil no institucional residente habitual en las cabeceras municipales de las principales capitales de departamento y las personas de 15 años y más. Se excluyen: cárceles, albergues infantiles, hogares geriátricos, conventos, seminarios, cuarteles guarniciones o estaciones de policía, y en general los denominados lugares especiales de alojamiento.

Se toma información en forma directa al jefe(a) de hogar y a cada una de las personas del hogar de 15 años y más (informantes directos), de acuerdo con su edad y sexo. Para las personas menores de 15 años la información correspondiente debe ser suministrada por el padre, la madre, o la persona del hogar que está a cargo de su cuidado cuando los padres no forman parte del hogar. Este procedimiento permite, adicionalmente, evitar que la entrevista se concentre en una sola persona.

La captura de datos se realiza a través de Dispositivos Móviles de Captura (DMC). Esto permite la detección automática de algunos errores de recolección, consistencia interna de la información y obtener datos con mayor precisión. Diariamente el apoyo informático de la sede o subsele, debe encargarse de realizar la transmisión de la información completa, capturada y depurada durante el operativo a DANE Central. Esta transmisión se efectúa a través del protocolo de comunicación de archivos FTP, previamente establecido por la Oficina de Sistemas de la entidad.

Figura 24. Diagrama de Contexto ECSC



Fuente: DANE

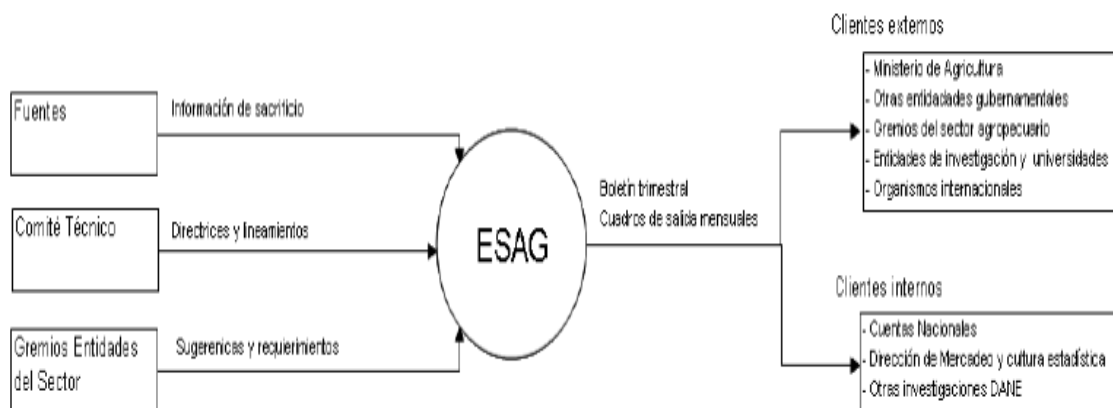
ENCUESTA DE SACRIFICIO DE GANADO - ESAG

El objetivo general Proporcionar información estadística sobre el número de cabezas, peso en pie y peso en canal, obtenido del sacrificio del ganado mayor (vacuno y bufalino) y menor (porcino, ovino y caprino) para el total nacional y distintos niveles de desagregación, con la oportunidad y confiabilidad requeridas, para facilitar el análisis y la planeación del subsector ganadero del país.

El alcance temático abarca la estimación del número de cabezas sacrificadas, su peso en pie y peso en canal desagregado por especie, sexo de ganado, destino de la carne en canal y procedencia del ganado sacrificado en las plantas de sacrificio (mataderos y frigoríficos), alcaldías, tesorerías municipales, oficinas de saneamiento ambiental o donde se reporta el sacrificio de ganado registrado.

Método de recolección formulario electrónico vía WEB, en donde las fuentes autodiligencian directamente la información y esta llega en tiempo real al servidor, posibilitando su visibilidad en las sedes y subsedes DANE y el nivel central.

Figura 25. Diagrama de Contexto ESAG



Fuente: DANE

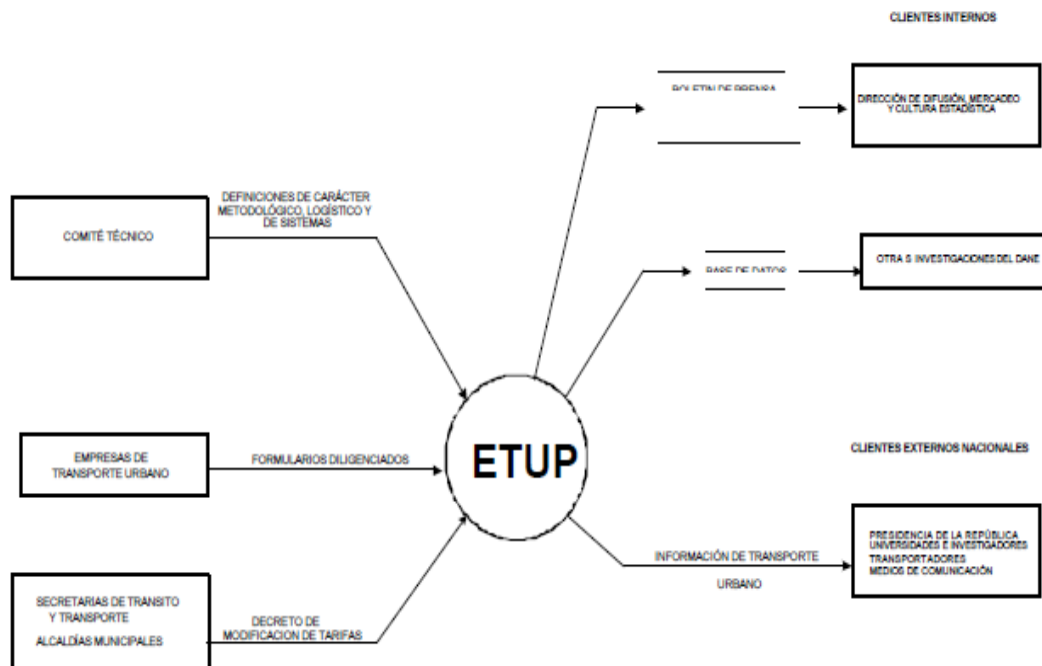
ENCUESTA DE TRANSPORTE URBANO DE PASAJEROS – ETUP

La encuesta se basa en el estudio del parque automotor y la movilización de pasajeros de las empresas legalmente constituidas que prestan el servicio, mediante el pago de una tarifa cuyo valor es determinado por las autoridades competentes en cada uno de los municipios (Secretaría de Tránsito y Transporte), por lo que la información que produce el DANE puede también servir como base para la negociación de las tarifas oficiales entre los transportadores y las autoridades competentes, en cada uno de los municipios con servicio de transporte urbano.

La población objetivo está compuesto por todas las empresas de transporte urbano automotriz legalmente constituidas, que operan en las 7 áreas metropolitanas y 16 ciudades capitales de departamentos.

El método de recolección es un Formulario auto diligenciado, con posibilidad de asesoría en los casos que se requieran, según la Dirección Territorial la distribución de los formularios es personal.

Figura 26. Diagrama de Contexto ETUP



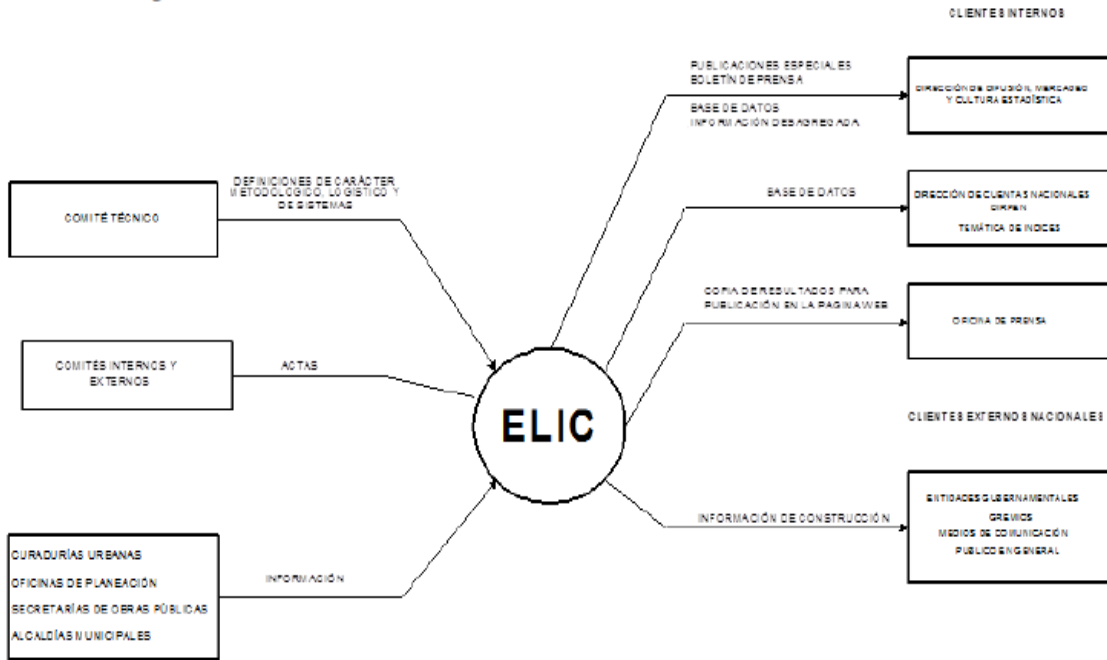
Fuente: DANE

ENCUESTA LICENCIAS DE CONSTRUCCIÓN - ELIC

Conocer el potencial de la actividad edificadora del país, a través de las licencias de construcción. Abarca las cifras sobre actividad edificadora se refiere a la construcción formal (urbana, suburbana y rural) en metros cuadrados aprobados, número de licencias otorgadas y número de unidades a construir.

Las Curadurías urbanas u oficinas de planeación dentro de los cinco (5) primeros días hábiles de cada mes suministran la información de Licencias de Construcción del mes inmediatamente anterior, de acuerdo con el Decreto 1469 de 2010, en un formulario expedido por el DANE.

Figura 27. Diagrama de Contexto ELIC

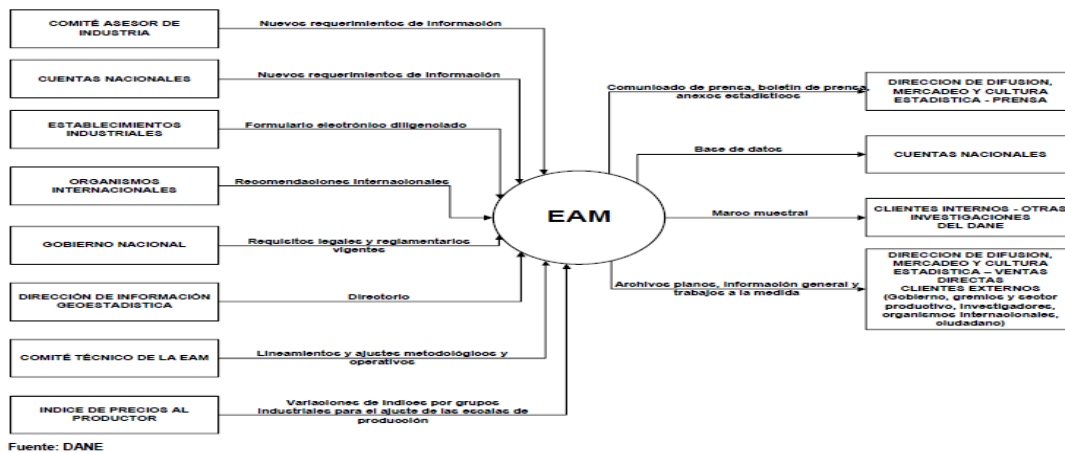


Fuente: DANE

ENCUESTA ANUAL MANUFACTURERA - EAM

La Encuesta Anual Manufacturera, es la investigación económica por medio de la cual el Departamento Administrativo Nacional de Estadística DANE, obtiene la información estadística del sector fabril colombiano, en cuanto a su estructura productiva, desarrollo y evolución.

Figura 28. Diagrama de Contexto EAM



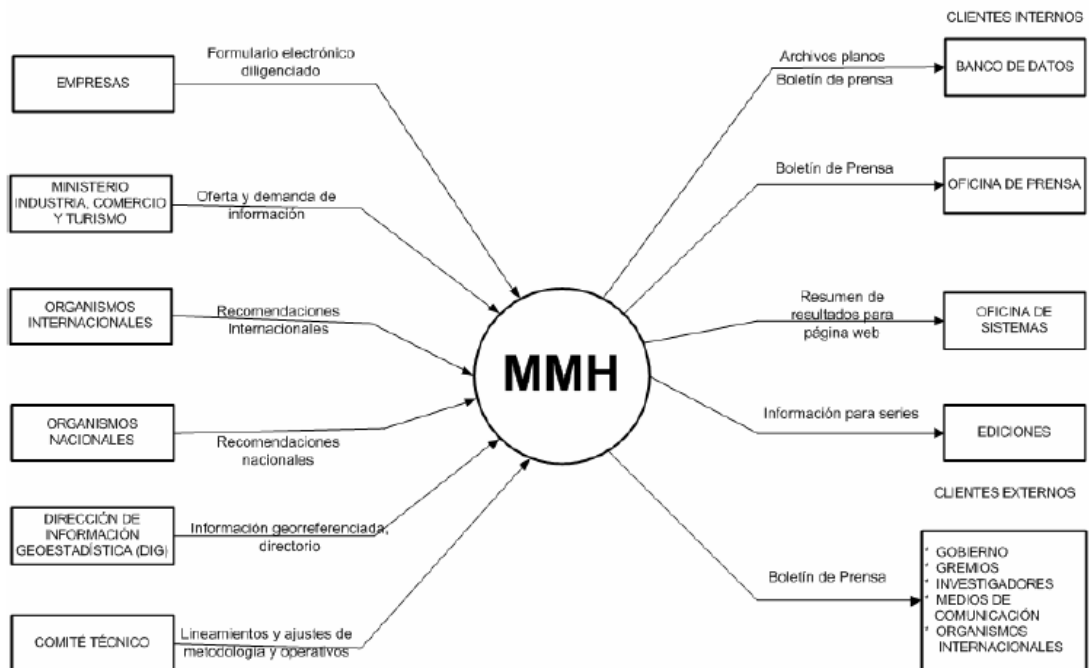
Fuente: DANE

Fuente: DANE

ENCUESTA MUESTRA MENSUAL DE HOTELES - EMMH

La Muestra Mensual de Hoteles es una investigación económica que permite conocer el comportamiento económico coyuntural del sector turístico nacional en cuanto a su desarrollo y evolución. Para ello se obtiene información necesaria para la estimación de los principales indicadores del sector de hoteles a nivel nacional.

Figura 29. Diagrama de Contexto MMH



Fuente: DANE

2.4 MARCO LEGAL

2.4.1 Leyes informáticas colombianas¹¹

Ley estatutaria 1266 del 31 de diciembre de 2008

Por la cual “dicta disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países”.

¹¹ UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. <http://www.unad.edu.co/gidt/index.php/leyesinformaticas>

Ley 1273 del 5 de enero de 2009. Delitos informáticos¹²

El 5 de enero, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Esta ley, se divide en dos capítulos: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

El capítulo primero hace referencia a los siguientes artículos.

- **Artículo 269A:** ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269B:** OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- **Artículo 269C:** INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- **Artículo 269D:** DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

²⁸<http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia#Ref4>

- **Artículo 269E:** USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269F:** VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269G:** SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- **Artículo 269I:** HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239, manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.

- **Artículo 269J:** TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Ley 1341 del 30 de julio de 2009. Mediante la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley estatutaria 1581 de 2012. Entra en vigencia el 17 de octubre del 2012, Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales.

2.4.2 Ley 603 de 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. El derecho de autor es una forma de propiedad privada que reconoce una protección jurídica especial al autor como creador de una obra literaria o artística, entendida como tal, toda expresión personal de la inteligencia manifestada en forma perceptible y original. La Ley 603 del 27 de julio de 2000, por la cual se modifica el artículo 47 de la Ley 222 de 1995, establece como una de las obligaciones de los representantes legales de las sociedades, incluir dentro de su informe de gestión, el grado de cumplimiento de la legislación referente al derecho de autor

2.4.3 Ley 734 de 2002. Numeral 21 y 22 del Art. 34, son deberes de los servidores Públicos “vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente”, y “responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización”¹³

2.4.4 Decreto 1377 de 2013. Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

2.4.5 Derechos de Autor

Ley 23 de 1982 Sobre Derechos de Autor

El derecho de autor es el conjunto de normas que protegen los derechos de los creadores de las obras. Comprende dos aspectos: los derechos morales y los derechos patrimoniales. Los primeros hacen referencia al conjunto de prerrogativas en virtud de las cuales el autor podrá reivindicar en todo tiempo la paternidad de la obra, oponerse a cualquier deformación que demerite la obra o su reputación, publicarla, o conservarla inédita, modificarla y a retirarla de circulación. Los derechos morales son intransferibles, irrenunciables e imprescriptibles.

Por su parte, los derechos patrimoniales son todas las facultades que le permiten al autor explotar económicamente la obra. El titular de tales derechos podrá realizar, autorizar o prohibir cualquier forma de utilización que se quiera hacer de la obra, tales como reproducirla, comunicarla al público, distribuirla, transformarla, ponerla a disposición, entre muchas otras. Su término de duración está limitado a la vida del autor más de 80 años después de su muerte.

¹³ SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea].
http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 TIPO DE INVESTIGACIÓN

El proyecto se desarrollará teniendo en cuenta la investigación participativa de tipo descriptiva, buscando recopilar toda la información referente a las buenas prácticas de seguridad informática que mitiguen el impacto que actualmente tiene la ingeniería social y que sea de vital importancia para los funcionarios y contratistas del Departamento Administrativo Nacional de Estadística, en la Territorial Centro Oriente - Subsede Cúcuta, así como también para la comunidad en general y que en algún momento pueda servir de apoyo a la hora de realizar proyectos que estén enfocados en el área de la seguridad informática e ingeniería social.

3.2 FUENTES DE INFORMACIÓN

3.2.1 Fuentes de información primaria. Las fuentes primarias de éste proyecto están constituidas por los investigadores, Magister, ingenieros del área de computación y tecnología de la información, al igual que el grupo de personas que hacen parte de la coordinación y ejecución del proyecto.

3.2.2. Fuentes de información secundaria. La información secundaria será toda aquella que esté consignada en libros, textos, revistas, periódicos, proyectos de grado y demás, artículos de Internet y otros, en relación con los temas que se requieran para el proyecto.

3.3 POBLACIÓN Y MUESTRA

La población que involucra este proyecto es el personal de las diferentes Áreas del Departamento Administrativo Nacional de Estadística - DANE. El cual está integrado por seis (6) Direcciones Territoriales a nivel Nacional y más de 800 servidores públicos.

La muestra la integra el Talento Humano del Departamento Administrativo Nacional de Estadística – DANE, Territorial Centro Oriente Subsede Cúcuta.

4. PRESENTACIÓN DE RESULTADOS

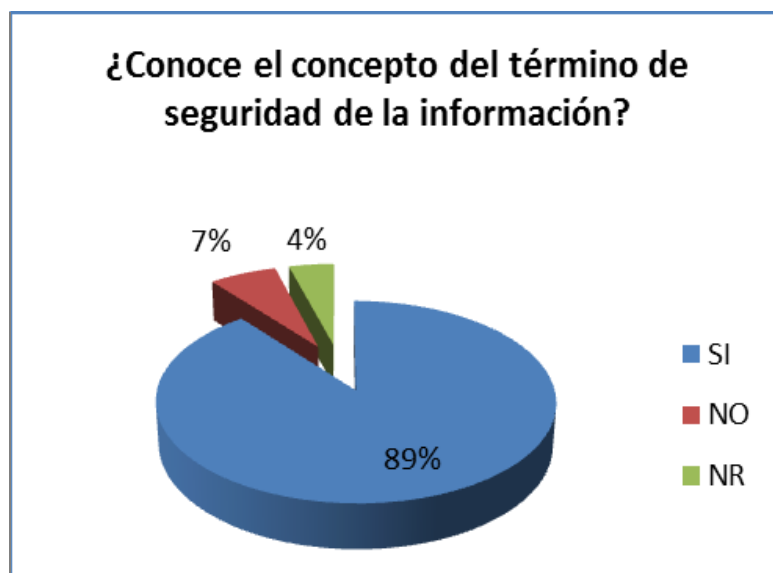
4.1 REALIZAR UNA AUDITORIA PASIVA PARA IDENTIFICAR FACTORES DE RIESGO QUE EXPONEN A LA INGENIERÍA SOCIAL EN EL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO SUBSEDE CÚCUTA.

Para el desarrollo de este objetivo realizo una auditoria pasiva utilizando los objetivos de control de ISO 27001:2013 que se encuentran asociados a la ingeniería social; como primer paso se utilizaron técnicas de recolección de información como lo son entrevistas, encuestas y observación la cual llevaron a los siguientes resultados.

Era importante identificar si el personal del Departamento Administrativo nacional de estadística territorial centro subsede Cúcuta se encuentra relacionado con la seguridad de la información; por lo tanto dentro de las preguntas realizadas de encuentran las siguientes:

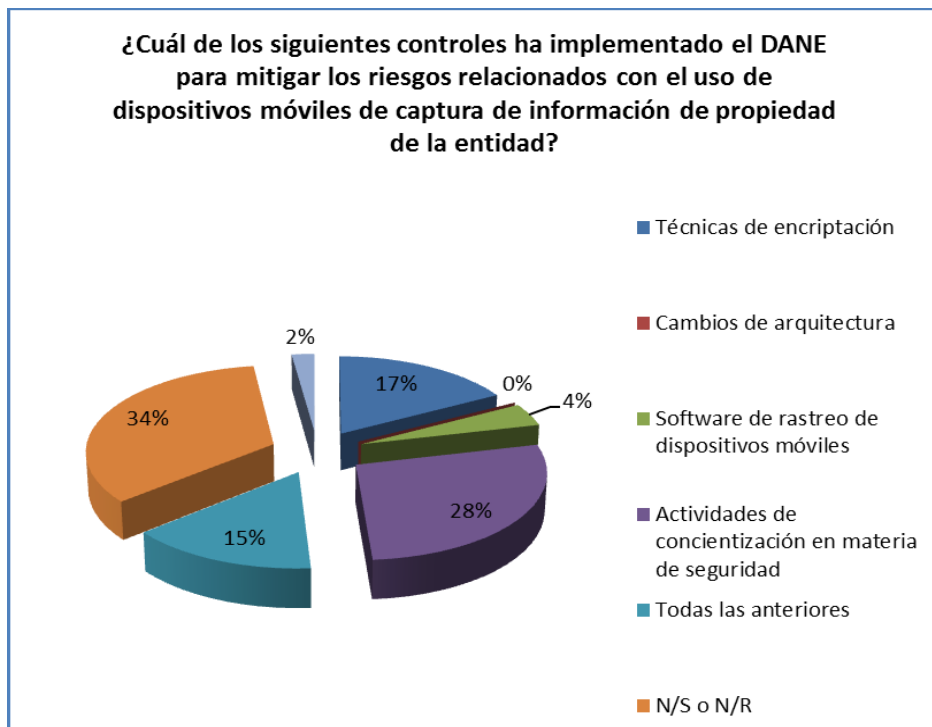
Aunque en la pregunta N° 1 el 89 % de la muestra encuestada dice que conoce el término de seguridad de la información, debido a la capacitación inicial que reciben al ingresar a la entidad, los tips informáticos que son publicados en la intranet entre otros. Un 11% de la muestra encuestada no responde o no conoce el término de seguridad de la información, lo cual conduce a que las capacitaciones no son lo suficientemente efectivas dejando una brecha amplia para ser vulnerada.

Grafica 1. Pregunta. N° 1- Encuesta Seguridad de la Información



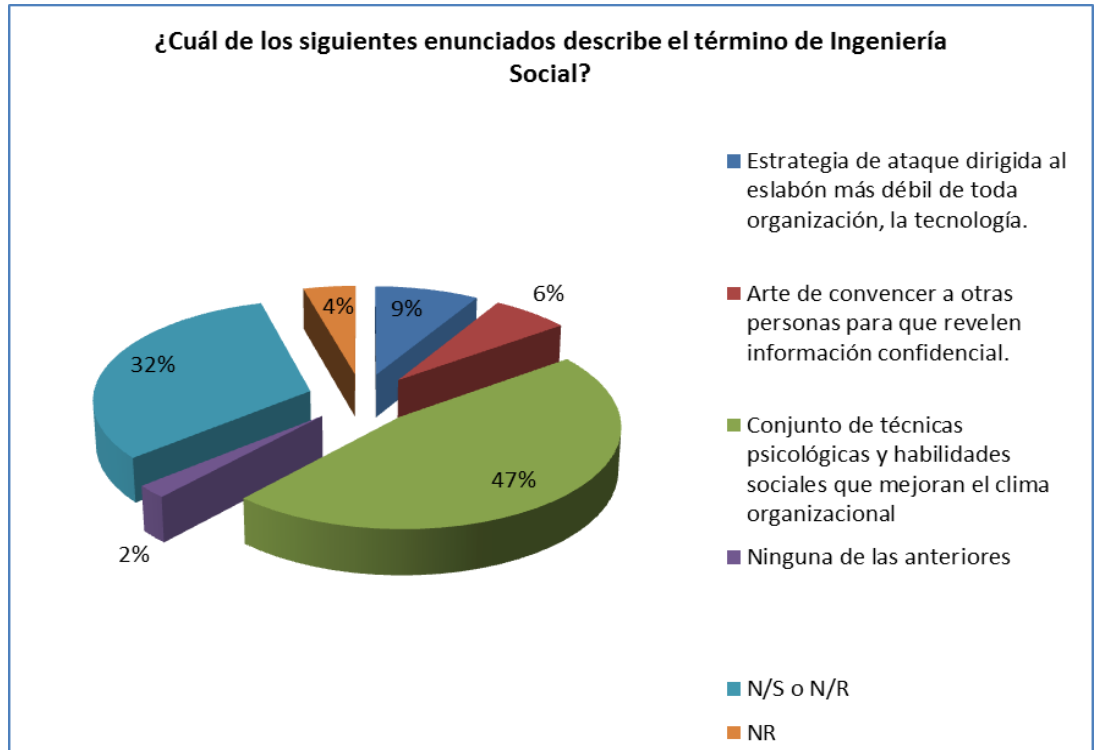
En la Grafica N° 3 se puede evidenciar que despues de que la empresa ha realizado capacitaciones e impartido boletines en la pagina web el 34% del personal no sabe o no responde si el DANE sub sede Cucuta a aplicado controles para mitigar los riesgos de la seguridad de la información. Sólo el 15 % de los encuestados tiene conocimiento de los controles que el DANE ha implementado para mitigar los riesgos latentes que a diario presenta el activo más importante.

Grafica 2. Pregunta. N° 3 - Encuesta Seguridad de la Información



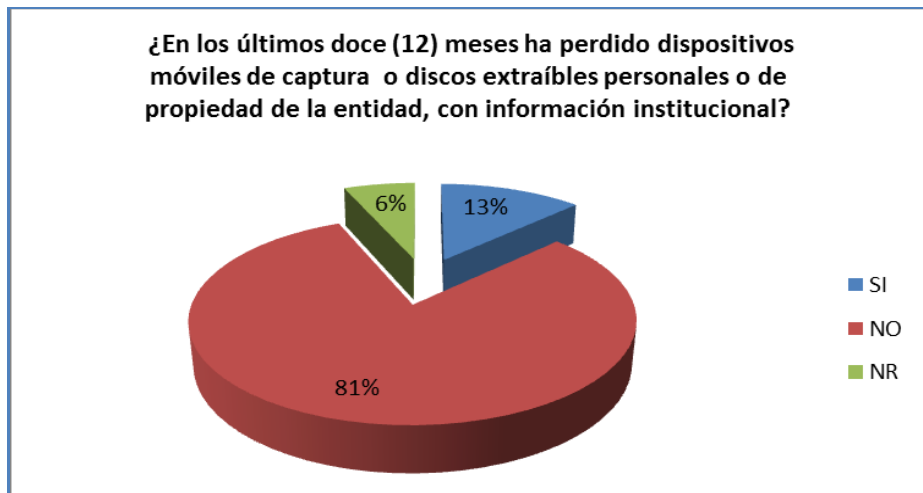
Con el fin de identificar si conocen que es ingeniería social se les realiza preguntas asociadas al término, en el cual sólo el 6% de los encuestados identifican el concepto correcto del término Ingeniería Social, y el otro 94% lo que representa una grave amenaza tanto para la entidad como a nivel personal. Para disminuir el riesgo de ser víctimas debemos combinar tanto la estructura tecnológica como la capacitación del talento humano. El desconocimiento del tema es la mayor ventaja que tiene un ingeniero social.

Grafica 3. Pregunta. N° 6 - Encuesta Seguridad de la Información



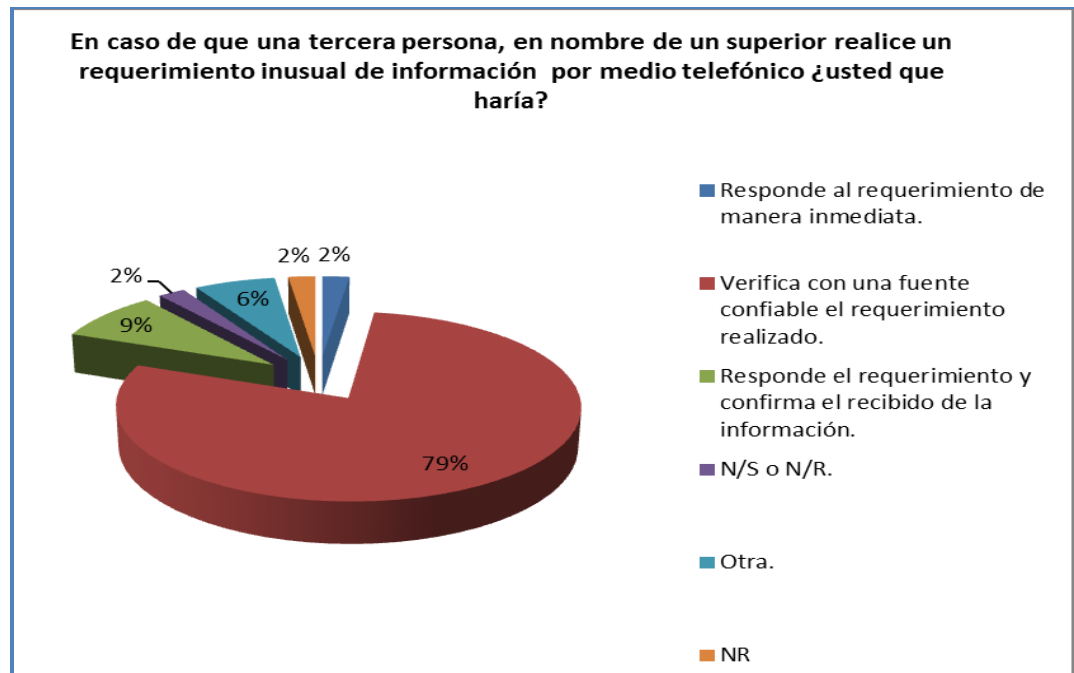
De acuerdo con el personal encuestado, el 13% reporta haber tenido perdida de un activo de la entidad con información institucional, y el 6% que no responde también se puede incluir, lo cual es de suma importancia prevenir este riesgo dentro del personal de la entidad, aunque es un porcentaje menor no se debe despreciar, si no tratar de reducir.

Grafica 4. Pregunta. N° 10- Encuesta Seguridad de la Información



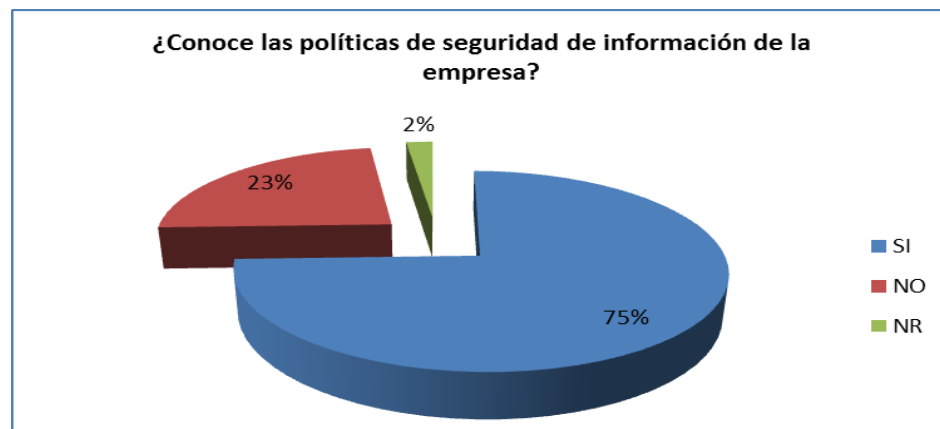
El 79 % de los encuestados respondieron el procedimiento que se debe hacer, aunque existe 21 % que realiza otro procedimiento, esto llevaría a un riesgo de pérdida de información y se debe estandarizar el lineamiento de verificar siempre con una fuente confiable el requerimiento realizado, antes de dar respuesta a este.

Grafica 5. Pregunta. N° 13- Encuesta Seguridad de la Información



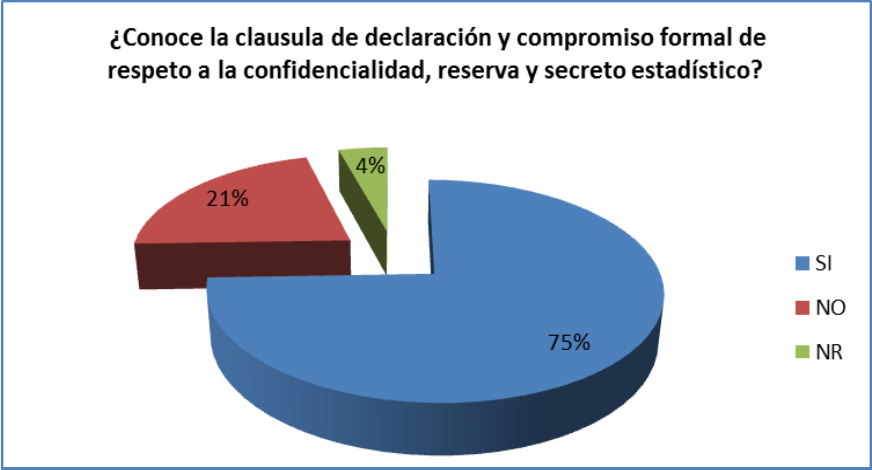
Aunque las políticas se encuentran publicadas en la intranet de la entidad y son socializadas en las capacitaciones de seguridad informática un porcentaje considerable de un 23 % del talento humano que contestó la encuesta las desconoce y un 2 % no dio respuesta a esta pregunta, y es de suma importancia que el 100% del personal conozca estas políticas.

Grafica 6. Pregunta. N° 14 - Encuesta Seguridad de la Información



El 21% y el 4% de la muestra desconocen de declaración y compromiso formal de respeto a la confidencialidad, reserva y secreto estadístico que se encuentra en el contrato laboral, lo que conlleva a que la información pueda ser divulgada incumpliendo la ley del habeas data.

Grafica 7. Pregunta. N° 18 - Encuesta Seguridad de la Información



4.2 IDENTIFICAR LOS OBJETIVOS DE CONTROL Y CONTROLES DE LA NORMA ISO/IEC 27001:2013 A LOS QUE SE ENCUENTRA EXPUESTOS EL DANE Y PUEDAN SER VULNERADOS POR INGENIERÍA SOCIAL.

Se tuvo en cuenta los objetivos de control los cuales pueden ser explotados por ingeniería social, se hace una breve descripción donde se argumenta el no cumplimiento del objetivo de control del DANE y como pueden ser vulnerados por la ingeniería social.

Núm.	Nombre	Descripción
5	Políticas de seguridad de la información	El DANE no cuenta con un oficial de seguridad de la información. Para el cual se debería definir un conjunto de políticas aprobada por la dirección y ofrecer la orientación de acuerdo con los requisitos, leyes y reglamentos de la empresa.
6	Organización de la seguridad de la información	Debido a que no existe un documento formal de política de seguridad de la información no existe definida su organización.
7	Seguridad de los recursos humanos	La entidad presenta una falencia en el departamento de recursos humanos en cuanto a la seguridad de la información, ya que las medidas impartidas no son suficientes para la seguridad correspondiente a la información.
8	Gestión de activos	Para el DANE es relevante que los medios que contienen información se deberían proteger contra acceso no autorizado o uso indebido. Por lo tanto se debe crear una política de gestión de activos que le permita al personal un debido manejo de los mismos.
9	Control de acceso	El departamento ha definido buenas prácticas para el control de acceso pero un porcentaje alto de los empleados no la conocen o no la cumplen, por lo que es de vital importancia exigir a los usuarios las prácticas para el uso de información de autenticación secreta y restringir el acceso no autorizado a sistemas y aplicaciones de acuerdo con la política de control de acceso de la organización.
10	Criptografía	Se necesita en el departamento desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información y asegurar el uso apropiado para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
11	Seguridad física y ambiental	La entidad cuenta con áreas seguras las cuales no cuentan con controles físicos de entrada y seguridad del equipamiento, por consiguiente se debe prevenir y

		proteger mediante controles apropiados para asegurar el acceso no autorizado, la pérdida, robo o daño de activos, la interrupción de operaciones y reducir los riesgos de amenazas y peligros del entorno.
12	Seguridad de las operaciones	Los procedimientos de operaciones están a disposición de todos los empleados que lo necesiten, pero la mayoría no los conoce o no los usan. Se deberían implementar controles de detección, de prevención y de recuperación, con la toma de conciencia de los usuarios, y asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos y pérdida de datos
13	Seguridad de las comunicaciones	Es necesario que el departamento identifique, revise y documente los requisitos de acuerdos de confidencialidad o no divulgación, por tanto debería asegurar y mantener la protección de la seguridad de la información de la entidad.
14	Adquisición, desarrollo y mantenimiento de sistemas	Para el DANE es de vital importancia asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida, por esta razón se deberían incluir los requisitos relacionados con seguridad de la información para los sistemas de información que ya existan o los nuevos que sean implementados.
16	Gestión de incidentes de seguridad de la información	En el departamento los servicios y sistemas de información han sido vulnerados, por tal razón se deben exigir a todos los empleados que los usan, que observen e informen cualquier debilidad o irregularidad en los servicios o sistemas de información para analizar y resolver incidentes de seguridad de la información y así reducir la posibilidad o el impacto de incidentes futuros
17	Aspectos de seguridad de la información en la gestión de continuidad de negocios	Para el DANE, la continuidad de la seguridad de la información es muy importante incluirla en los sistemas de gestión de continuidad de negocio ya que las falencias en seguridad de la información dentro del DANE se ha visto reflejados en la muestra de la encuesta realizada, por ello se debe documentar, implementar y mantener procedimientos, procesos y controles para asegurar el nivel de continuidad para la seguridad de la información.
18	Cumplimiento	Los directivos del DANE deberían revisar periódicamente el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad con las políticas y normas de seguridad

		de la información, para así evitar el incumplimiento de las obligaciones legales, estatutarias de reglamentación o contractuales relacionadas con seguridad de la información.
--	--	--

4.3 DEFINIR LOS CRITERIOS DEL MANUAL DE PREVENCIÓN DE RIESGOS DE ATAQUES DE INGENIERÍA SOCIAL PARA EL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO ORIENTE SUBSEDE CÚCUTA.

Para el desarrollo del tercer objetivo se define una estructura formal donde se contemplan los criterios del manual de prevención de riesgos de ataque de ingeniería social al departamento administrativo nacional de estadística territorial centro subsede Cúcuta, como se describe a continuación.

1. TITULO
2. ALCANCE
3. OBJETIVO DEL MANUAL
4. CAMPO DE LA APLICACIÓN
5. INTRODUCCIÓN
6. DESCRIPCIÓN DE LA ESTRUCTURA DE LA ORGANIZACIÓN
7. QUÉ ES INGENIERÍA SOCIAL
8. OBJETIVOS DE LA INGENIERÍA SOCIAL
9. FASES DE LA INGENIERÍA SOCIAL
 - 9.1 Recopilación de Información
 - 9.2 Selección de la Víctima
 - 9.3 El Ataque
10. TÉCNICAS DE INGENIERÍA SOCIAL
 - 10.1 Human-Based Social Engineering
 - 10.2 Computer-Based Social Engineering
 - 10.3 Mobile-Based Social Engineering
11. ARMAS DEL INGENIERO SOCIAL
12. QUE HACER DURANTE O DESPUÉS DE UN ATAQUE
13. CONTRAMEDIDAS
14. TIP DE DEFENSA
15. USO DEL CORREO ELECTRONICO
16. USO DEL NAVEGADOR/ACCESO A INTERNET
17. USO DEL SERVICIO DE MENSAJERÍA
18. CUIDADOS CON LAS CONTRASEÑAS
19. CUIDADOS CON LAS REDES INALÁMBRICAS
20. CUIDADOS CON MEDIOS DE ALMACENAMIENTO EXTRAIBLES

1. MANUAL DE PREVENCIÓN DE RIESGOS DE ATAQUES DE INGENIERÍA SOCIAL PARA EL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA TERRITORIAL CENTRO ORIENTE SUBSEDE CÚCUTA

2. ALCANCE

El alcance de este manual es contribuir con el control y prevención de los riesgos a los que está expuesto la ingeniería social, puesto que la misma tecnología lo ha convertido en un sistema vulnerable y la mejor herramienta de combatirlo es el conocimiento y la preparación para contrarrestar los ataques.

3. OBJETIVO DEL MANUAL

Orientar al personal del Departamento Administrativo Nacional de Estadística Territorial Centro Oriente Subsede Cúcuta para la prevención de riesgos de ataques de ingeniería social.

4. CAMPO DE LA APLICACIÓN

Este manual está dirigido al Departamento Administrativo Nacional de Estadística Territorial Centro Oriente Subsede Cúcuta, para su respectiva aplicación y toma de conciencia apropiado del personal.

5. INTRODUCCIÓN

El presente manual tiene como propósito contar con una guía clara y específica que garantice la óptima operación y desarrollo de la prevención de riesgos de ataques de la Ingeniería Social a través de la práctica de obtener información confidencial y de la manipulación de usuarios legítimos, puesto que la ingeniería social también es llamada el “arte del engaño” y los Ingenieros sociales son como "actores” que asumen un papel y tratan de representarlo de la mejor manera posible.

Comprende en forma ordenada, secuencial y detallada las armas del ingeniero social, que hacer durante o después de un ataque, contramedidas, tips de defensa, uso del correo electrónico, uso del navegador/acceso internet, uso del servicio de mensajería, cuidado con las contraseñas, cuidado con las redes inalámbricas, cuidados con medios de almacenamiento extraíble y así promover el buen desarrollo administrativo del departamento administrativo nacional de estadística territorial centro oriente subsede Cúcuta.

6. DESCRIPCIÓN DE LA ESTRUCTURA DE LA ORGANIZACIÓN



Fuente: DANE

7. QUE ES INGENIERÍA SOCIAL

Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

- Arte de convencer a otras personas para que revelen información confidencial.
- Estrategia de ataque dirigida al eslabón más débil de toda organización, las personas.
- Conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente para obtener información de terceros.
- Manipulación Inteligente de la tendencia natural de las personas a ayudar.
- Dentro de la naturaleza humana, el instinto de conservación incluye la confianza en el otro también con el fin de desarrollar nuestra especie.

8. OBJETIVO DE LA INGENIERÍA SOCIAL

La ingeniería social también es llamada el “arte del engaño”.

Los Ingenieros sociales son como "actores" que asumen un papel y tratan de representarlo de la mejor manera posible.

Todo con el fin de:

- Obtener la mayor cantidad de información posible sobre su objetivo.
- Comprometer la confidencialidad de la información de la manera más sutil.
- Robo de identidad.
- Infiltrarse para Robar Información y otros activos.
- Conocerlos planes estratégicos de la competencia.

9. FASES DE LA INGENIERÍA SOCIAL

9.1 Recopilación de información:

El atacante Investiga sobre la compañía o persona objetivo, haciendo uso de redes sociales, páginas web, llamadas, correos etc...

9.2 Selección de la víctima:

- Recepcionistas
- Personal de mesa de ayuda
- Soporte Técnico
- Vendedores/Personal del área comercial
- Administradores de Sistemas
- Usuarios y clientes

9.3 El ataque:

Establecer contacto, relaciones con la víctima y explotar la relación construida.

10. TÉCNICAS DE INGENIERÍA SOCIAL

10.1 HUMAN-BASED SOCIAL ENGINEERING

- Suplantación de un usuario Legítimo:

Por ejemplo: "Atacante: Buenos días Soy xxxx del área de estadísticas vitales, olvide mi contraseña, puedes ayudarme (HelpDesk)".

- Suplantación de Personal Técnico:

Por Ejemplo: "Atacante: Buenos días mi nombre es xxxxx de la mesa de ayuda, estamos realizando una verificación del software instalado en los PC, ¿por favor me facilita la IP de su equipo, Usuario y contraseña, de igual manera verificamos que los permisos de acceso remoto estén habilitados?"

- Eavesdropping:

Escuchar Pasivamente las conversaciones de los empleados con el fin de extraer de esta información sensible.

- Shoulder Surfing:

Mirar sobre el Monitor ó sobre el Hombro de un empleado/Victima con el fin de identificar información confidencial como: user names, passwords, etc.

- Dumpster Diving o ¿Qué hay en nuestra basura?:

“Nadar”, Buscar en la basura de la organización: documentos impresos, manuscritos, informes, agendas, notas etc.; que puedan contener información confidencial.

- Listados Telefónicos.
- Organigramas.
- Memorandos Internos.
- Manuales de Políticas de la Compañía.
- Agendas en Papel de Ejecutivos con Eventos y Vacaciones.
- Manuales de Sistemas.
- Impresiones de Datos Sensibles y Confidenciales.
- “Logins”, “Logons” y a veces... contraseñas.
- Listados de Programas (código fuente).
- Discos extraíbles (CD – ROM, DVD, SD, USB).
- Papel Membreteado y Formatos Varios.
- Hardware Obsoleto.

- In Person: Visitar Físicamente A La Víctima

- Autorización de Tercera persona:

Suplantar a un empleado que llama a otro en nombre de su jefe solicitando información confidencial.

- Tailgating (chupar rueda):

Seguir a una persona con acceso autorizado a un área aprovechando que aún no se ha cerrado la puerta.

- Reverse Engineering:

Hacerse pasar por alguien de autoridad ante la víctima con el fin de tener acceso a la información.

- Piggy Backing:

Solicitar el acceso al vigilante con el pretexto de que olvido su llave de acceso.

10.2 COMPUTER-BASED SOCIAL ENGINEERING

- Mensajes Hoax:

Mensajes de Correo que incitan al usuario a comprometer sus propios activos.

- Ventanas Emergentes / pop-ups:

Ventanas y formularios flotantes que motivan al usuario a hacer click sobre estos y así descargar software malicioso.

- Cadenas de mensajes:

Mensajes de correo electrónico que es reenviado por los mismos usuarios con el fin de construir bases de datos de contactos

- Correo no deseado/SPAM:

Mensajes de correo electrónico que podrían incluir código malicioso o motivar a los usuarios a ser víctimas de estafas

- Mensajería Instantánea:

Charlas de nuevos contactos que pretenden ganar confianza a través de perfiles falsos y comprometer la tecnología de la víctima a través de software malicioso.

- Phising/Spearphising:(Dirigido A Una Persona En Particular):

Ataques de suplantación de sitios web propagados principalmente a través de mensajes de correo electrónico.

- Principales ataques de Ingeniería Social apoyada en tecnología:

- Redes sociales
- fakeprofiles, chats, etc.
- Email-basedcyberattacks
- Hoaxes
- Phising
- Software Malicioso
- Troyanos
- Backdoors
- Bots

10.3 MOBILE-BASED SOCIAL ENGINEERING

La ingeniería social también ha permeado las plataformas de computación móvil debido a la masificación de las APPs y la penetración de las mismas a las organizaciones.

- **Apps Maliciosas:**
Malware que se comercializan como software espía, servicios y contentProviders maliciosos.
- **Apps Legítimas reempaquetadas:**
Aplicaciones móviles legítimas troyanizadas.
- **Fake Security Apps:**
Aplicaciones que se muestran como antivirus y que comprometen al sistema operativo
- **Ataques vía SMS/MMS:**
Aplicaciones que propagan malware a través de los servicios de mensajería de la red celular.

11. ARMAS DEL INGENIERO SOCIAL

- **Adoptar Rasgos de un rol:**
Con el Objetivo de hacer creer a las demás personas que se es, el rol que se está interpretando e inferir credibilidad, el atacante exhibe Vestido, peinado, habla, comportamientos, joyas, utiliza lenguaje técnico de la entidad, menciona nombres de jefes y compañeros de trabajo.

Por ejemplo: Si vemos a una persona muy bien vestida con un estetoscopio, asumimos que este es un médico.

Si vemos a un hombre vestido de ejecutivo asumimos que es inteligente, centrado y de confianza.

- **Credibilidad:**
Generar confianza en la víctima. Normalmente es el primer paso en la mayoría de los ataques de Ingeniería social.

Tres (3) métodos para construir credibilidad:

- Decir algo en contra de su interés real:
Por ejemplo: "Escribe tu contraseña, pero no me la digas (Shouldersurfing), recuerda que nunca por ningún motivo debes decirle a nadie tu contraseña. “
- Advertirle a la víctima sobre un hecho (provocado por el mismo atacante):
Por ejemplo: Informarle a la Víctima que debido a un fallo de red, no se podrá tener acceso a los servidores de la empresa.

- Resolverle un problema a la víctima, (Uno que el mismo atacante causo)

Por ejemplo: después de bloquear el acceso a un servicio, habilitárselo a la víctima.

- Vulnerabilidad aprovechada: No verificar la veracidad de la información que recibimos ni las credenciales de la otra persona.

- **Lograr que la Víctima adopte un rol:**

Manipular a la persona con el fin de que tome el papel que se desea.

Normalmente se pretende identificar el papel con que más “a gusto” se siente la víctima y que pueda ser aprovechado por el atacante.

Se logra que la víctima tome un "papel de colaboración", una vez aceptado el rol será difícil que la persona se niegue a ayudar.

Es muy probable que las personas acepten roles positivos apoyados por un poco de adulación y motivación.

Por ejemplo: "Usted parece ser muy buena persona y un empleado que quiere a la empresa, por favor facilítame el acceso al centro de comunicaciones"

- Vulnerabilidad Aprovechada: Agrado de sentirse elogiado y admirado por las demás personas.
- Objetivo: Eliminar la resistencia de la víctima a colaborar.

- **Impulso de la Conformidad:**

La táctica de “Una cosa más”, comenzar con una charla que incluya algunas preguntas inofensivas y nada sospechosas y dejar la pregunta que comprometería la confidencialidad para el final. Con el fin de que sea contestada con confianza y pase desapercibida por la víctima.

- Vulnerabilidad aprovechada: Bajar la guardia y asumir que la otra persona es confiable.
- Objetivo: Pasar desapercibido el intento de acceder a información privilegiada.

- **Ganarse la simpatía:**

Hacer cumplidos y halagos, aprovecharse de su buen físico e incluso Hacer pensar que se comparten sus gustos y se tienen intereses similares a los de la víctima.

Por ejemplo: "No sabía que en esta empresa contrataran mujeres tan hermosas como tú", "He escuchado muchas cosas buenas sobre su desempeño laboral y su compromiso con la empresa".

- Vulnerabilidad aprovechada: La exaltación del ego de las víctimas y el gusto por que las otras sean como nosotros, tengan nuestras mismas aficiones, etc. eso nos genera confianza y facilita su colaboración.
- Objetivo: Caerle bien a la víctima partiendo de la premisa que siempre decimos "si" a las peticiones de las personas que nos caen bien.
- Miedo: hacer creer a su víctima que algo malo está a punto de pasar y que ese desastre inminente puede evitarse si la víctima sigue las instrucciones del atacante.

Por ejemplo: - Se le informa a la víctima que está a punto de perder datos muy importantes a menos que acepte instalar un parche en el servidor.

- Se le informa a la víctima que hay evidencias de que desde su pc se realizó una acción indebida y que está a punto de ser despedida a menos que le permita a la "buena persona" del Helpdesk tener acceso a su PC para eliminar la evidencia.
- Impresionara un directivo o a un empleado de alto rango con la exigencia de "urgente" y con la insinuación al subalterno de que el no cumplimiento de la orden podrá costarle el puesto.
- Vulnerabilidad aprovechada: Falta de verificación y Credibilidad de cualquier hecho relatado por cualquier otra persona.
- Objetivo: Mostrarse ante la víctima como la solución al problema.
- Reactancia: En psicología, es una reacción negativa que experimentamos cuando sentimos que nos han arrebatado nuestra capacidad de elección y nuestras libertades.

En esta situación, el individuo pierde el sentido de la perspectiva por el deseo inmenso de recuperar eso que ha perdido es más fuerte.

Por ejemplo: "Mesa de ayuda: Debido a la migración de cuentas en el servidor de archivos, su cuenta será suspendida durante 2 semanas,... pero si requiere con urgencia la restauración de sus archivos facilítenos su usuario y contraseña“.

- Vulnerabilidad aprovechada: Falta de verificación de la situación y de Deseo Humano de querer recuperar los bienes.
- Objetivo: Obtener la colaboración gustosa de la víctima.

12. QUE HACER DURANTE O DESPUÉS DE UN ATAQUE.

En caso de que el personal de la empresa detecte algo sospechoso, debe informar el incidente siguiendo los lineamientos.

Confirmar los requerimientos inusuales de información con fuentes Confiables.

Mantener siempre la cordialidad, amabilidad y simpatía con los clientes internos y externos, así como mantener el tacto para identificar posibles atacantes que quieren captar información confidencial.

13. CONTRAMEDIDAS

Los controles que pueden emplearse para disminuir la efectividad de los ataques ingeniería social deben ser considerados como parte de las políticas de seguridad de la Información y pueden ser:

- Orientados a la seguridad física:
 - Identificar al personal de la empresa, con uniformes y Carnets
 - Acompañar a los visitantes, nunca dejarlos solos
 - Destrucción total de documentos que contienen información sensible o confidencial / no solo a la basura.
 - Contratar Personal experto en seguridad física.
 - Implementar políticas de escritorio limpio.
 - Siempre verificar la identidad de los visitantes.
 - Etc.

- Orientados a la seguridad Lógica:
 - Restringir la publicación de información que pueda ser usada en contra de la empresa.
 - Restringir el acceso en horas No laborales al personal de la empresa.
 - Generar trazabilidad a las acciones de los usuarios.
 - Usar un buen antimalware actualizado incluso en los móviles.
 - Usar criptografía.
 - Usar contraseñas complejas (en cuanto a longitud y Formato)
 - Cambiar contraseñas con mucha periodicidad.
 - No repetir contraseñas usadas con anterioridad.
 - Bloquear las cuentas al tercer intento.
 - Usar contraseñas en los salvapantallas.
 - Usar responsablemente el correo electrónico.
 - Deshabilitar los puertos físicos (USB, Firewire, etc.)
 - Hacer uso de servidores de Logsy de sistemas IPS/IDS.

14. TIP DE DEFENSA

- Mantenga una actitud cautelosa y revise constantemente sus tendencias de ayudar a personas que no conoce.
- Verifique con quien habla, especialmente si le están preguntando por contraseñas, datos del personal de la empresa u otra información sensitiva.

- Al teléfono, obtenga nombres e identidades (identificación, por ejemplo). Corrobórelos y llámelos a su pretendida extensión.
- No se deje intimidar o adular para terminar ofreciendo información.
- Sea cauteloso (de nuevo, no paranoico) en las encuestas, concursos y ofertas especiales vía internet, teléfono y correo electrónico y convencional. Estas son formas comunes de obtener direcciones de correo electrónico, contraseñas y otros datos personales.

15. USO DEL CORREO ELECTRONICO

- Correo Electrónico institucional:

- Es de propiedad de la empresa.
- Esta bajo nuestra administración y responsabilidad.
- Medio de comunicación oficial.

- Correo Electrónico Personal:

- Pertenece al usuario
- Usado para enviar y recibir mensajes privados
- No debe usarse para enviar o recibir información institucional.

Principales cuidados:

- Consultar el correo institucional solo desde (dentro de la empresa):

- La computadora del puesto de trabajo.
- Tablet PC Personal
- Smartphone Personal
- A través de VPN

- Si la empresa hace uso de un webmail considerar:

- Verificar la autenticidad del URL
- Cerrar la sesión al finalizar actividades o al retirarse de su puesto de trabajo.
- Hacer uso de contraseñas robustas

- No descargar adjuntos de mensajes de correo que provengan de cuentas:

- Desconocidas.
- Nuestra propia cuenta.
- No reenviar cadenas de mensajes.
- No diligenciar formularios ni instrumentos enviados a través del correo electrónico.
- Por ningún motivo NUNCA envíe nombres de usuario, contraseñas, números de cuenta, números de tarjetas débito ni crédito, pines, claves, etc a través de mensajes de correo.

16. USO DEL NAVEGADOR/ACCESO A INTERNET

Principales cuidados:

Siempre verificar la autenticidad del sitio web antes de ingresar sus credenciales de acceso:

- Preste atención a la barra de dirección e identifique caracteres extraños en el URL.
- Verifique la presencia de un certificado digital y cerciórese de su validez.
- Revise el contenido de las páginas del sitio y trate de identificar elementos que puedan ser falsos.
- No visite sitios web que su sistema antimalware considere maliciosos.
- Nunca habilite la función de «Recordar Contraseñas» en ningún formulario de autenticación.
- Tener precaución con los resultados arrojados por los buscadores.
- Evitar los enlaces sospechosos.
- No hacer click sobre enlaces de las ventanas emergentes.
- No descargar, ni instalar software de ninguna clase.
- Siempre leer detenidamente los mensajes de advertencia de las cajas de dialogo.
- Si tiene dudas antes de ejecutar alguna acción sobre un sitio web sospechoso apóyese en el personal de TI de la organización.

17. USO DEL SERVICIO DE MENSAJERÍA

Principales cuidados:

Nunca acepte la invitación de usuarios desconocidos a través de los servicios de mensajería (CHAT) como:

- Lotus
- Open fire/Spark
- Gtalk
- Messenger/Skype
- Yahoo messenger
- Facebook Messenger.
- Etc.

Nunca digite credenciales, números de tarjetas, cuentas bancarias; en general ningún tipo de información confidencial debe ser transferida a través de los servicios de mensajería instantánea.

No acepte adjuntos enviados a través del servicio de chat, mucho menos enviados por desconocidos.

No brinde información sobre su sistema computacional a ninguna persona vía IM.

No informe sobre sus actividades laborales ni las de sus compañeros de trabajo a través del IM.

No envíe fotografías tomadas dentro de su compañía a nadie a través de ningún medio electrónico.

18. CUIDADOS CON LAS CONTRASEÑAS

Las contraseñas son usadas para validar a los usuarios de un sistema informático, por lo tanto estas deben ser consideradas de uso privado

No use la misma contraseña para todas las cuentas.

No comparta las contraseñas con nadie (Información Confidencial).

No revelar una contraseña por teléfono a NADIE.

No envíe una contraseña en un mensaje de correo electrónico.

No revele una contraseña al jefe.

No divulgue una contraseña delante de otros.

No indicar el formato de una contraseña (por ejemplo, "mi nombre" familiar).

No divulgar una contraseña en encuestas o formularios de seguridad.

No compartir una contraseña con los miembros de la familia.

No revelar una contraseña a los colaboradores mientras esté de vacaciones

Si le exigen una contraseña, haga referencia a este documento o hágalos llamar a algún responsable de Seguridad de la Información.

No use la funcionalidad de "Recordar la Contraseña" de algunas aplicaciones (por ejemplo, Outlook, Messenger, etc...).

No escriba o guarde las contraseñas en cualquier parte de la oficina.

No guarde las contraseñas en NINGUN archivo de computadora (incluso Teléfonos Móviles o dispositivos similares) sin encriptación.

Cambie por lo menos una vez las contraseñas cada 2 meses.

Si sospecha que una contraseña ha sido descubierta, informe al responsable de Seguridad de la Información y cambie todas las contraseñas.

Las contraseñas robustas tienen las características siguientes:

- Contienen caracteres con mayúscula y minúscula (por ejemplo, un-z, UN-Z)
- Tienen dígitos y caracteres de puntuación junto con letras por ejemplo, 0-9! @ # \$ % ^ & * () _+ | -= \ { } []: "; '<>?. /)
- Son por lo menos ocho caracteres alfanuméricos.
- No son unas palabras en cualquier idioma, dialecto, jerga, etc.,
- No están basadas en la información personal, los nombres de familia, etc.,

Las contraseñas nunca deben apuntarse o guardarse en línea.
Cree contraseñas que puedan recordarse fácilmente.

Una manera de hacer esto es crear una contraseña basada en un título de canción u otra frase. Por ejemplo, la frase podría ser: "Esta Puede Ser Una Manera de Recordar" y la contraseña podría ser: "EpS1MdR!" o "eP5UmDr" o alguna otra variación.

19. CUIDADOS CON LAS REDES INALÁMBRICAS

No se conecte a redes inalámbricas desconocidas con equipos de la empresa.

Si requiere el acceso haga uso del servicio de VPN.

No acceda a ningún servicio de la organización a través de redes inalámbricas públicas o sin protección.

No consulte su correo electrónico, ni envíe información sensible haciendo uso de una red inalámbrica pública.

Deshabilite la interface inalámbrica (WIFI/Bluetooth, etc) mientras no esté conectado a ninguna red wireless.

No comparta ningún archivo o recurso mientras esté conectado a la red wireless.

20. CUIDADOS CON MEDIOS DE ALMACENAMIENTO EXTRAIBLES

Se conoce como medios de almacenamiento extraíbles a:

- Memorias Flash (USB).
- Discos Duros externos.
- CD / DVD / Blu-rays.
- Memorias Micro SD MMC
- Cámaras digitales.
- Teléfonos Móviles.

No permita que desconocidos conecten memorias flash o discos externos a su computadora.

Si es necesario copiar un archivo a su disco duro verifique la salud de la memoria/ disco externo/DVD con su sistema antivirus/Antimalware.

Lea con detenimiento todos los mensajes de advertencia de su sistema cuando haga uso de medios extraíbles.

Ante cualquier sospecha de que su sistema ha sido comprometido comuníquese con el área de seguridad de la Información.

5. CONCLUSIONES

Se realizó una auditoria pasiva para identificar los factores de riesgo que exponen a la ingeniería social en el departamento administrativo nacional de estadística territorial centro subsede Cúcuta, identificando la importancia de la seguridad de la información, se logró identificar las vulnerabilidades y falencias que fomentan el riesgo de la perdida, daño o acceso no autorizado en los servicios y sistemas de información dentro del departamento, estas vulnerabilidades se vieron reflejadas en la encuesta realizada al personal de la entidad, en el cual se identificaron los controles necesarios que permitirán reducir el impacto de la ingeniería social en la seguridad de la información.

Se tomaron algunos objetivos de control y controles de la norma ISO 27001:20013, mostrando en una tabla los mismos y con relación a la necesidad encontrada en el Departamento Administrativo Nacional de Estadística Territorial Centro Oriente subsede Cúcuta a la falta de un manual de prevención de riesgos de seguridad de la información se tomó como base la norma, ya que permite una integración adecuada con la normatividad y métodos utilizadas por el departamento, además constituye un beneficio indispensable de la utilización de un método de seguridad basado en entornos internos y externos.

Con los criterios del manual de prevención de riesgos de ataques de ingeniería social para el Departamento Administrativo Nacional de Estadística Territorial Centro Oriente Subsede Cúcuta, el cual es una herramienta de Ingeniería Social, elaborado para permitir la comprensión de los usuarios, y sensibilizar al personal acerca de la ingeniería social. Se realizan ejemplos, con lo cual se pretende mostrar cuales son los pasos que hace un “delincuente” para robar información. Por tal motivo es un asunto de alta relevancia para cualquier persona y aún más para cualquier entidad. Es de vital importancia seguir las buenas prácticas de seguridad de la información, tanto a nivel físico como lógico.

BIBLIOGRAFÍA

Carmen Lucia Pedraza Garzon, V. A. (2011). Guías Prácticas para uso de Técnicasde Ingeniería Social con la Herramienta Set Incluida en la Distribución Backtrack 4 R2. Guías Prácticas para uso de Técnicasde Ingeniería Social con la Herramienta Set Incluida en la Distribución Backtrack 4 R2. Bogotá DC, Colombia.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION ISO/IEC 27000.
www.iso27000.es.

Nederlandsch Economisch-Historisch Archief: J.C. van Marken - Biografisch portret bio en Wiki francesa: Émile Cheysson William Howe Tolman (1909):

Social Engineering New York Times: Dr. Tolman Sails on His Mission. David Östlund (2007): The Business Career of the Terminology of Social Engineering 1894-1910

Ann-Katrin Hatje (2007): Female Social Engineering and Its Philanthropic Roots

Carl Marklund (2007): Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA

SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea]. http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

<http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia#Ref4>

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADISTICA – DANE. Ficha metodológica - Modelo Funcional. www.dane.gov.co

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. <http://www.unad.edu.co/gidt/index.php/leyesinformaticas>

William Hálaby CISSP, 2014
<http://isc2capitulocolombia.org/portal/images/documents/ISO27001-2013ISC2ColombiaChapter.pdf>

ANEXOS

ENCUESTA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Conocer el nivel de vulnerabilidad en seguridad de la información que tiene el personal del Departamento Administrativo Nacional de Estadística DANE – Territorial Centro Oriental - Subsede Cúcuta.

Le agradecemos se tome el tiempo necesario para responder toda la encuesta y siéntase en entera libertad para contestarla de manera sincera.

Responda toda la encuesta y ante todo sea honesto, de ello depende que podamos identificar fortalezas y debilidades en el área de seguridad de la información.

Indique el cargo.

- Supervisor de contrato
- Coordinador de Campo
- Supervisor o Analista
- Sensibilizador, Recolector, Monitor
- Aérea administrativa y Servicios Generales
- Soporte Informático

RECUERDE QUE LA INFORMACION SUMINISTRADA ES DE CARÁCTER CONFIDENCIAL

Marque con una (X)

1. ¿Conoce el concepto del término de seguridad de la información?

SI () NO ()

2. ¿De los activos relacionados a continuación cual considera usted que el más importante para la organización?

- a) Dispositivos Móviles de Captura
- b) Centro de Comunicaciones
- c) Información
- d) Equipos de computo

3. ¿Cuál de los siguientes controles ha implementado el DANE para mitigar los riesgos relacionados con el uso de dispositivos móviles de captura de información de propiedad de la entidad?

- a) Técnicas de encriptación
- b) Cambios de arquitectura
- c) Software de rastreo de dispositivos móviles
- d) Actividades de concientización en materia de seguridad
- e) Todas las anteriores
- f) N/S o N/R

4. ¿Cuáles de los siguientes controles ha implementado el DANE para mitigar los riesgos del uso de redes sociales en equipos de propiedad de la entidad?

- a) Uso limitado a redes sociales
- b) Restricción del uso de redes sociales
- c) Ajustes en las políticas de seguridad informática
- d) Monitoreo de internet
- e) N/S o N/R

5. ¿Cuáles de las siguientes acciones ha tomado su organización para controlar la fuga de información confidencial?

- a) Definición de una política específica en cuanto a la clasificación y manejo de información confidencial.
- b) Implementación de mecanismos de seguridad adicionales para proteger la información (ej. encriptación)
- c) Bloqueo/restricción de uso de ciertos componentes de hardware (ej. puertos USB, puertos Firewire)
- d) Campañas de sensibilización
- e) Todas las anteriores
- f) Ninguno
- g) N/S o N/R

6. ¿Cuál de los siguientes enunciados describe el término de Ingeniería Social?

- a) Estrategia de ataque dirigida al eslabón más débil de toda organización, la tecnología.
- b) Arte de convencer a otras personas para que revelen información confidencial.
- c) Conjunto de técnicas psicológicas y habilidades sociales que mejoran el clima organizacional
- d) Ninguna de las anteriores
- e) N/S o N/R

7. ¿En los últimos doce (12) meses la entidad ha realizado capacitación en seguridad de la información?

SI NO N/S o N/R

(Si su respuesta es NO ó NS/NR salte a la pregunta N° 10)

8. ¿En los últimos doce (12) meses ha asistido capacitación en seguridad de la información?

SI NO

(Si su respuesta es NO salte a la pregunta N° 10)

9. ¿Considera que las capacitación en seguridad de la información que ha recibido en los último doce (12) meses tiene aplicación en el cumplimiento de sus funciones?

SI NO

10. ¿En los últimos doce (12) meses ha perdido dispositivos móviles de captura o discos extraíbles personales o de propiedad de la entidad, con información institucional?

SI NO

11. ¿Conoce los lineamientos o instrucciones a seguir en caso de siniestro o pérdida de un bien de la entidad?

SI () NO ()

12. ¿Cuál de los siguientes enunciados describe el término phishing?

a) () Es un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas por medio de ingeniería social caracterizado por adquirir información confidencial de forma fraudulenta.

b) () Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.

c) () Es un malware que tiene la propiedad de duplicarse a sí mismo, a diferencia de un virus el gusano no precisa alterar los archivos de programas, si no que reside en la memoria y se duplica.

d) () Lo ha escuchado en los medios de comunicación pero desconoce el concepto.

e) () N/S o N/R

13. En caso de que una tercera persona, en nombre de un superior realice un requerimiento inusual de información por medio telefónico ¿usted qué haría?

a) () Responde al requerimiento de manera inmediata.

b) () Verifica con una fuente confiable el requerimiento realizado.

c) () Responde el requerimiento y confirma el recibido de la información.

d) () N/S o N/R.

e) () Otra. Cual_____

14. ¿Conoce las políticas de seguridad de información de la empresa?

SI () NO ()

15. Consulta el correo electrónico (Personal ó institucional), ò comparte archivos con información confidencial haciendo uso de una red inalámbrica pública.

SI () NO ()

16. Revela la contraseña a los compañeros de trabajo mientras está de comisión o vacaciones.

SI () NO ()

17. Cada cuanto tiempo realiza el cambio de contraseñas de correo electrónico (Institucional o Personal).

a) () Una vez al mes.

b) () Una vez cada dos (2) meses.

c) () Una vez al trimestre.

d) () Una vez al semestre.

e) () Una vez al año

f) () Nunca la ha cambiado.

18. ¿Conoce la cláusula de declaración y compromiso formal de respeto a la confidencialidad, reserva y secreto estadístico?

SI () NO ()

19. ¿Ha compartido con los compañeros del equipo de trabajo información confidencial que ha llegado a conocer por causa o con ocasión del ejercicio del cargo?

SI () NO ()

20. ¿Conoce las sanciones que ocasiona la divulgación de información o material sujeto a reserva, secreto o Confidencialidad estadística que llegue a conocer por causa o con ocasión de la relación con la entidad?

SI () NO ()