RESUMEN – TRABAJO DE GRADO

AUTORES	**KARLA JULIANY CASTRO GUERRERO**
FACULTAD	**INGENIERIAS**
PLAN DE ESTUDIOS	**INGENIERIA DE SISTEMAS**
DIRECTOR	**ESP. LUIS ANDERSON CORONEL**
TÍTULO DE LA TESIS	**FORMULACIÓN DE CONTROLES BASADOS EN LA NORMA NTC- ISO 27002 PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL COMITÉ DEPARTAMENTAL DE CAFETEROS DEL CAUCA.**

RESUMEN
(70 palabras aproximadamente)

LA INFORMACION ES EL ACTIVO MAS IMPORTANTE DE TODA ORGANIZACIÓN, LA REALIZACIÓN DE ESTE PROYECTO TIENE COMO OBJETIVO PRINCIPAL; FORMULAR UNA SERIE DE CONTROLES DE SEGURIDAD, BASADOS EN LA NORMA ISO 27002, QUE PERMITAN PROTEGER LA INFORMACION DEL COMITÉ DE CAFETEROS DEL DEPARTAMENTO DEL CAUCA, CONTRA CUALQUIER TIPO DE AMENAZAS FÍSICAS O LÓGICAS A LAS QUE PUEDA ESTAR EXPUESTA DICHA ENTIDAD, ES POR ELLO QUE EL DESARROLLO DEL PROYECTO AYUDARA A MEJORAS CONSIDERABLES DENTRO DE LA MISMA.

CARACTERÍSTICAS

PÁGINAS: 84	PLANOS:	ILUSTRACIONES:	CD-ROM:**1**

FORMULACIÓN DE CONTROLES BASADOS EN LA NORMA NTC- ISO 27002 PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL COMITÉ DEPARTAMENTAL DE CAFETEROS DEL CAUCA

KARLA JULIANY CASTRO GUERRERO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2015

FORMULACIÓN DE CONTROLES BASADOS EN LA NORMA NTC- ISO 27002 PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL COMITÉ DEPARTAMENTAL DE CAFETEROS DEL CAUCA

KARLA JULIANY CASTRO GUERRERO

Trabajo de grado para obtener el título de Ingeniero de sistemas

Director del Proyecto
Esp. LUIS ANDERSON CORONEL
Ingeniero en sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2015

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

INTRODUCCION

Desde mediados del siglo XX la tecnología ha invadido apresuradamente aspectos en los que el hombre se desarrollapolítica, cultural, económica y socialmente. Gracias al mismo desarrollo del hombre se hace indispensable implementar toda clase de políticastecnológicas dentro de las entidades públicas y privadas, con el fin de optimizar el desempeño de cada una de ellas.

Para dicho objetivo es necesario conocer todas y cada una de las herramientas que la tecnología permite utilizar; en beneficio de garantizar la seguridad de la información canalizándola hacia un máximo rendimiento.

Aunque es difícil garantizar que no existan riesgos, siempre será importante minimizar las amenazas de robo oaccesos no autorizados, como también los aspectos relacionados con la disponibilidad de la información,que puedan afectar de una u otra manera la integridad, confidencialidad y veracidad de los datos. Para la tarea de reducir dichas amenazas es importante implementar un conjunto de controles que nos permitan suprimir los posibles riesgos que pretendan afectar la seguridad de la organización.

Este proyecto tiene como fin brindar al Comité Departamental de Cafeteros del Cauca un documento con los controles basados en la norma ISO 27002 que les permita proteger la información y los equipos que la procesan y almacenan. En primera instancia se estudia cada dominio de la norma, con el fin de determinar los objetivos de control necesarios para un funcionamiento eficaz y confiable. Por último se genera al Comité, un informe detallado de todas inconsistencias que se presentan en su organización y las posibles soluciones a cada una de ellas, permitiéndoles decidir sobre su aplicación.

1. TITULO

FORMULACIÓN DE CONTROLES BASADOS EN LA NORMA NTC- ISO 27002 PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL COMITÉ DEPARTAMENTAL DE CAFETEROS DEL CAUCA.

1.1 PLANTEAMIENTO DEL PROBLEMA

El Comité Departamental de Cafeteros del Cauca, como ente representativo de la Federación Nacional de Cafeteros de Colombia en el departamento del Cauca se encuentra constituido por varias áreas de trabajo que se encargan de garantizar el bienestar de aproximadamente 95 mil familias caficultoras.

Para el cumplimiento de sus objetivos el Comité lleva a cabo una serie de programas que orientan al caficultor del departamento del Cauca en sus labores de producción, ayudando a suplir sus necesidades básicas. Lo que implica un manejo permanente de información, asociada a los datos personales, ubicación, estado de cafetales, y pago de producción, a través de diferentes aplicaciones web que están interconectados al Sistema de Información Cafetera SICA, generando un riesgo de la seguridad de la información, que podría acarrear pérdidas para el comité.

La información que se manipula es altamente confidencial, y los controles adoptados para la seguridad de la información son casi nulos, las contraseñas de acceso no se cambian periódicamente, no se hacen mantenimientos preventivos, antivirus desactualizados, entre otros, inadecuado manejo de las copias de seguridad, que han hecho que en la entidad ya se hayan presentado situaciones preocupantes de pérdida de información, sin consecuencias graves hasta ahora pero duplicando el trabajo mientras se recupera dicha información y con una alta posibilidad de que sigan ocurriendo estos incidentes, que más adelante si podrían dejar secuelas de mayor envergadura.

1.2 FORMULACIÓN DEL PROBLEMA

¿Un conjunto de controles basados en la norma NTC – ISO 27002 garantizará al Comité Departamental de Cafeteros del departamento del Cauca, la seguridad de su información?

1.3 OBJETIVOS DE LA INVESTIGACION

1.3.1 Objetivo General. Formular controles basados en la norma NTC – ISO 27002 para la seguridad de la información del Comité Departamental de Cafeteros del Cauca.

1.3.2 Objetivos Específicos.

Realizar un diagnóstico del manejo de la información en el Comité.

Analizar la norma ISO 27002, para determinar y establecer los aspectos aplicables al comité Departamental.

Elaborar un documento entregable al Comité, de los controles encontrados durante el análisis, permitiéndoles hacer mejoras basadas en las recomendaciones propuestas.

1.4 JUSTIFICACIÓN

Con el transcurrir del tiempo se han gestado miles de alternativas e innovaciones con el fin de satisfacer las necesidades de la sociedad consumista, tanto que la Información se ha convertido en el activo más importante de toda empresa, organización o entidad, por esto se vuelve delicado el manejo de la información, pues cualquier fallo en la seguridad física y del entorno, en el desarrollo y mantenimiento de sistemas de información o en un acceso no autorizado pondría en riesgo la seguridad de la información.

Para proteger este Activo se hace necesaria la implementación de políticas de seguridad que garanticen la fiabilidad de la Información, generando confianza y tranquilidad para quienes quieren proteger dicha Información. De este escenario es consciente el Comité Departamental de Cafeteros del Cauca, quienes reconocen que no se están llevando a cabo los controles para la seguridad de su información y desean que mediante este proyecto se pueda conocer la situación real por la que atraviesa su organización para que se puedan tomar las medidas necesarias.

Por lo tanto surge la idea de formular controles basados en la norma NTC – ISO 27002 para la seguridad de la información del Comité Departamental de Cafeteros del Cauca, que les permita obtener un diagnóstico real de su organización y la propuesta de los controles requeridos para asegurar ese activo tan valioso como es la información.

1.5 HIPOTESIS

Con la formulación de controles basados en la norma ISO 27002, se garantizará en gran medida la Seguridad de la Información en el Comité Departamental de Cafeteros del Cauca.

1.6 DELIMITACION Y ALCANCES

1.6.1 Geográficas. Este proyecto fue desarrollado en el Comité Departamental de Cafeteros del Cauca (Popayán).

1.6.2 Temporal. Este proyecto se llevó a cabo en un tiempo de 8 semanas.

1.6.3 Conceptual. En el desarrollo del proyecto se tuvieron en cuenta conceptos como: seguridad, información, controles, riesgos, ISO 27002, ISO 27001, sistemas de información, copias de seguridad, antivirus, etc.

1.6.4 Operativa. Este documento basado en la Norma ISO 27002 que contiene controles para la seguridad de la información del Comité Departamental de Cafeteros del Cauca, es de libre aplicación para todos los empleados de planta, contratistas y aprendices del Sena que ejercen una labor en el Comité.

2. MARCO DE REFERENCIA

2.1 MARCO HISTORICO

2.1.1 Reseña Histórica de la Federación Nacional de Cafeteros[1]. En 1927 los cafeteros colombianos se unieron con el fin de crear una organización que los representara nacional e internacionalmente, y que velara por su bienestar y el mejoramiento de su calidad de vida. Así nació la Federación Nacional de Cafeteros de Colombia (FNC), considerada hoy como una de las ONG rurales más grandes del mundo. La Federación es una entidad sin ánimo de lucro, y no está afiliada a ningún partido político.

Desde 1927 ha sido el principal gremio de Colombia, con presencia en todas las zonas rurales donde se produce café en el país. Su eje central es el productor de café y su familia, de forma que su negocio sea sostenible, que las comunidades cafeteras fortalezcan su tejido social y que el café colombiano siga siendo considerado como el mejor del mundo.

Nuestra Federación representa a más 563 mil familias cafeteras que a través de los años se ha caracterizado por ser profundamente democrática, desarrollando una estructura de representación gremial para tomar decisiones que consulten las prioridades de la base del gremio, los productores de café y sus familias. De esta forma los mismos productores colombianos de café llegan a los consensos necesarios para definir programas y acciones para el beneficio común.

La Federación está conformada por los siguientes órganos y niveles jerárquicos:

Congreso Nacional de Cafeteros.
Comité Nacional de Cafeteros
Comité Directivo
Comités Departamentales de Cafeteros
Comités Municipales de Cafeteros

2.1.2 Comité Departamental de Cafeteros.[2]. Existe un Comité Departamental de Cafeteros en cada una de las capitales de los departamentos cuya producción cafetera excede el dos por ciento (2%) del total nacional. Funciona como órgano permanente integrado por seis (6) miembros principales con sus respectivos suplentes, los cuales son elegidos democráticamente en cada departamento en las circunscripciones uninominales creadas para tal efecto; además, son los mismos delegados al Congreso Cafetero.

[1]FEDERACION NACIONAL DE CAFETEROS. Quienes somos. Bogotá. Colombia [en línea]. Disponible en http://www.federaciondecafeteros.org/particulares/es/quienes_somos
[2]FEDERACION NACIONAL DE CAFETEROS. Comités departamentales. Bogotá. Colombia [en línea]. http://www.federaciondecafeteros.org/particulares/es/nuestros_caficultores/comites_departamentales/

Entre sus principales funciones están la de organizar y orientar el gremio en el respectivo departamento y la de ejecutar los distintos planes y programas para la región. El periodo de los miembros del Comité será de cuatro años.

2.1.3 Comité Departamental de Cafeteros del Cauca[3]. Es un ente representativo de la Federación Nacional de Cafeteros de Colombia. Esta organización representa nacionalmente a más de 95 mil familias caficultoras del departamento del Cauca y vela por su bienestar y el mejoramiento de su calidad de vida. Es una entidad sin ánimo de lucro, y no está afiliada a ningún partido político.

Su misión es "Asegurar el bienestar del caficultor colombiano a través de una efectiva organización gremial, democrática y representativa" y su visión "Consolidar el desarrollo productivo y social de la familia cafetera, garantizando la sostenibilidad de la caficultora y el posicionamiento del café de Colombia como el mejor del mundo".

2.1.4 A nivel Internacional. Desarrollo de políticas de seguridad informática e implementación de cuatro dominios en base a la Norma 27002 para el área de hardware de la empresa Uniplex Systems S.A. en Guayaquil.[4]

2.1.5 A nivel Nacional. Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001.[5]

Caracterización de Procesos de Gestión de TI basados en COBIT 5 y mapeo con ISO27002, ITIL, CMMI DEV, PMBOK, para la implementación en la industria Editorial Colombiana, apoyando el proceso de transformación digital. [6]

---

[3]FEDERACION NACIONAL DE CAFETEROS. Nuestro comité. Bogotá. Colombia. [en línea]. http://cauca.federaciondecafeteros.org/fnc/nuestro_comite/

[4]LAMILLA R, Erick A. PATIÑO S, José R. Desarrollo de políticas de seguridad informática e implementación de cuatro dominios en base de la norma 27002 para el área de hardware en la empresa UniplezSystem S.A. Escuela Superior Politécnica del Litoral "ESPOL". Guayaquil. Ecuador. Descripción [en línea].
https://www.dspace.espol.edu.ec/bitstream/123456789/5247/1/Desarrollo%20de%20Pol%C3%ADticas%20de%20Seguridad%20Inform%C3%A1tica%20e%20Implementaci%C3%B3n.pdf

[5]BUITRAGO E, Johana C. BONILLA P, Diego H. MURILLO V, Carol E. Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información – SDSI, en el sector de laboratorios de análisis microbiológicos, vasado en ISO 27001. Bogotá. Colombia. 2012 [en línea] Disponible en: http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

[6]MUÑOZ SERNA, Rodrigo y MARTINEZ ARIAS, Mario Alberto. Caracterización de Procesos de Gestión de TI basados en COBIT 5 y mapeo con ISO27002, ITIL, CMMI DEV, PMBOK, para la implementación en la industria Editorial Colombiana, apoyando el proceso de transformación digital. Disponible en la Web y de acceso libre. Universidad ICESI, Santiago de Cali. 2012.
https://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/70260/1/caracterizacion_proceso_gestion.pdf

Evaluación mediante el estándar ISO 27001 de la seguridad física y lógica de la infraestructura tecnológica de la Clínica San José S.A.S de la ciudad de Barrancabermeja – Santander.[7]

Sistema de administración de controles de seguridad informática basado en ISO/IEC 27002.[8] Este artículo presenta una plataforma web abierta denominada SGCSI que permite apoyar la gestión de controles de seguridad de la información de acuerdo con el estándar ISO 27002. Tras la evaluación comparativa del uso de la plataforma por parte de expertos y aprendices en seguridad, se pudo evidenciar su efectividad en la auditoría sobre el cumplimiento de los 32 objetivos de control establecidos por la norma.

2.1.6 A nivel Regional. Plan de gestión de la seguridad de la información de la biblioteca ArgemiroBayona de la Universidad Francisco de Paula Santander Ocaña, mediante la aplicación de la norma ISO 27001 y técnicas de Ethical Hacking.[9]

Guía para la seguridad basada en la norma ISO/IEC 27002, para la dependencia división de sistemas de la Universidad Francisco De Paula Santander Ocaña.[10]

2.2 MARCO CONTEXTUAL

Esta investigación se llevó a cabo en el Comité Departamental de Cafeteros del Cauca ubicado en la ciudad de Popayán (Cauca, Colombia), Donde se estudió el manejo de la información en el Comité de Cafeteros y con respecto a ese manejo se analizó la norma ISO 27002, con la cual se pudo determinar aspectos aplicables a la seguridad de la información del Comité, finalmente se reunió toda la información obtenida en un documento que les permitirá hacer mejoras a dicho manejo.

---

[7]MARULANDA PADILLA, Henry. Evaluacion mediante el estándar ISO 27001 de la seguridad física y lógica de la infraestructura tecnológica de la clínica San José S.A.S de la ciudad de Barrancabermeja. Barrancabermeja Santander. Julio 2014. Disponible en: http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/180.

[8]FRANCO, Diana C. y GUERRERO, Cesar D.Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002. Disponible en la Web y de acceso libre. Universidad de los llanos, Villavicencio; Universidad Autónoma Bucaramanga, Colombia. Agosto de 2013. http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf

[9]LOBO PARRA, Leonard David; OVALLOS OVALLOS, JesúsAndrés y SIERRA GOMEZ, Ana María. Plan de gestión de la seguridad de la información de la biblioteca Argemiro Bayona de la Universidad Francisco de Paula Santander Ocaña, mediante la aplicaion de la norma iso 27001 y técnicas ethical hacking. Universidad Francisco de Paula Santander Ocaña. Diciembre, 2013. Disponible en: http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/325/1/25095.pdf

[10]MOLINA RINCON, Erica Lorena; RODRIGUEZ ALVAREZ, Oscar Humberto; SANCHEZ DELGADO, Yalide y VERGEL NUÑEZ, John Alexander. Guía para la seguridad basada en la norma iso/iec 270002, para la dependencia división de sistemas de la Universidad Francisco de Paula Santander Ocaña. Universidad Francisco de Paula Santander Ocaña. Julio, 2014. Disponible en: http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/439/1/25830.pdf

La protección de los datos es responsabilidad de cada empleado, pero es el Director Ejecutivo del Comité de Cafeteros el directamente responsable de este activo, así como de los registros de la organización y la aplicación de controles que genera un alcance considerable a un 100% de la seguridad de la información,

2.3 MARCO CONCEPTUAL

Los siguientes términos y definiciones fueron aplicados en el desarrollo de este proyecto.

Acceso autorizado: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Acceso físico: Restringen la entrada y salida de personal, equipos y medios de áreas como edificios, centros de datos o cuartos de servidores.

Amenaza: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática o los Elementos de Información.[11].

Análisis de Riesgos: Proceso sistemático de identificación de fuentes, estimaciónde impactos y probabilidades y comparación de dichas variables contra criteriosde evaluación para determinar las consecuencias potenciales de pérdida deconfidencialidad, integridad y disponibilidad de la información.

Autorización: Garantizar que todos los accesos a datos y/o medios, cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

Backup's: Son copias de respaldo o de seguridad del sistema o de los datos, que puede ser utilizada en caso de producirse un fallo generalizado, caída del sistema, o el daño o eliminación accidental de archivos. Gracias a la información contenida en el Backup's, se podrá restaurar el sistema al estado en que se encontraba en el momento de realizar la copia de seguridad.

Confidencialidad: es la garantía de que la información sea accesible solo aquellas personas autorizadas a tener acceso a ella.

Contraseña: Conjunto de caracteres que permite el ingreso a un recurso informático.

[11] ERB, Markus. Gestión de Riesgo en la Seguridad Informática. Amenazas y Vulnerabilidades. España. 3h. [en línea]. http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Controles. [12]Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

Clasificación general de los controles _

Controles Preventivos: Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.
Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones.
Sistemas de claves de acceso.

Controles detectivos: Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.
Ejemplo: Archivos y procesos que sirvan como pistas de auditoría.
Procedimientos de validación.

Controles Correctivos: Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

Control de acceso: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Correo electrónicoó"E-mail". Es un software que puede utilizarse para el envío y recepción de mensajería entre usuarios, entendiendo por mensajería cualquier texto, archivo, programa, etc.

Desastre o Contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Disponibilidad: Es la garantía de que los usuarios autorizados tengan acceso a lainformación y a los recursos relacionados con ella cada vez que se requiera.

[12] SERRANO CEDILLOS, Leticia Esmeralda. El rol de la auditoria computarizada como herramienta de confiabilidad en la información contable. Universidad Dr. JoseMatias Delgado, antiguo Cuscatlan. El Salvador, Cantroamerica.Nobiembre, 2006.

Estructura organizacional: Puede ser definida como las distintas maneras en que puede ser dividido el trabajo dentro de una organización para alcanzar luego la coordinación del mismo orientándolo al logro de los objetivos.

Filtración de datos: Sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados.

Hardware: El hardware está formado por los componentes físicos. Es la parte "dura", es decir, las partes que configuran la máquina y que le dan una serie de características.

Impacto: Daño potencial sobre un sistema cuando una amenaza se presenta[13].

Información. Es un conocimiento transferible, recopilable y procesable que se representa mediante datos almacenados en un soporte.Profundizando un poco más se puede decir que la información es toda aquella documentación en poder de una organización, independientemente de la forma que adquiera o los medios por los cuales se distribuya o almacene (cintas, papel, audio u otras alternativas), que como otros de los activos, tiene un valor para la organización y por consiguiente debe ser protegida en debida forma, de los diferentes amenazas que la pongan en riesgo.

Integridad: es la salvaguarda de la exactitud y totalidad de la información y losmétodos de procesamiento de la misma.

ISO/IEC 27002: El objetivo del estándar es brindar información a los responsables de laimplementación de seguridad de la información de una organización. En él sedefinen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. La norma subraya laimportancia de la gestión del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellasque sean relevantes.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Políticas: Es el conjunto de grandes orientaciones y lineamientos que guían las acciones a desarrollar por la institución, a fin de mejorar su funcionamiento; directrices que se traducen en los objetivos y metas que un sistema se propone alcanzar dentro de un futuro determinado, asociados a la indicación de los medios más generales que deberán ser utilizados para alcanzarlos[14].

---

[13]UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Modulo Evaluación de la Seguridad de la Información. Ocaña. Colombia. 2012. 65h.

[14] MANUAL DE SEGURIDAD. [En línea]. [15 Mayo 2013]. Disponible En: https://euskadi.net/r47-contbp2z/es/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf

Políticas de Seguridad de la Información. Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes.

Procedimiento de seguridad: Proporcionan las instrucciones detalladas para llevar a cabo las tareas relacionadas con la seguridad de la información. Los procedimientos tienen un ámbito reducido de actuación y tienen siempre carácter operativo. Los procedimientos complementan los estándares de seguridad aportando la operativa necesaria para cumplirlas.

Recursos informáticos: son aquellos componentes de hardware y software talescomo: servidores (de aplicaciones y de servicios de red), estaciones de trabajo,equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios dered de datos y bases de datos, entre otros, los cuales tienen como finalidadapoyar las tareas académicas y administrativas necesarias para el buenfuncionamiento y la optimización del trabajo al interior de la empresa.

Riesgos informáticos.[15]Existe una incertidumbre constante por la presencia de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos, como equipos informáticos, periféricos, instalaciones, programas de cómputo, etc.

Es importante en toda organización contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático.

Tipos de Riesgos.

1. **Riesgo de integridad:** Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares, y en múltiples momentos en todas las partes de las aplicaciones; no obstante estos riesgos se manifiestan en los siguientes componentes de un sistema:

   Interface del usuario**:** Los riesgos en esta área generalmente se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; teniendo en cuenta sus necesidades de trabajo y una razonable segregación de obligaciones. Otros riesgos en esta área se relacionan

[15]AUDITORIA DE SISTEMAS. Riesgos Informáticos. Colombia. [en línea]. Disponible en: http://auditoriadesistemas.galeon.com/productos2223863.html

a controles que aseguren la validez y completitud de la información introducida dentro de un sistema.

Procesamiento: Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles defectivos y preventivos que aseguran que el procesamiento de la información ha sido completado. Esta área de riesgos también abarca los riesgos asociados con la exactitud e integridad de los reportes usados para resumir resultados y tomar decisiones de negocio.

Procesamiento de errores: Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada/proceso de información de errores (Excepciones) sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.

Administración de cambios: Estos riesgos están asociados con la administración inadecuadas de procesos de cambios de organizaciones que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.

Información: Estos riesgos están asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos.

2. **Riesgos de relación:** Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (Información y datos correctos de una persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).

3. **Riesgos de acceso:** Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: Los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información. Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:

   Administración de la información: El mecanismo provee a los usuarios acceso a la información específica del entorno.

   Entorno de procesamiento: Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.

Redes: En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.

Nivel físico: Protección física de dispositivos y un apropiado acceso a ellos.

4. **Riesgo de utilidad:** Estos riesgos se enfocan en tres diferentes niveles de riesgo:

   Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
   Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
   Backups y planes de contingencia controlan desastres en el procesamiento de la información.

5. **Riesgos de infraestructura:** Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (servicio al cliente, pago de cuentas, etc.

6. **Riesgos de seguridad general:** Los estándar IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:

   Riesgos de choque de eléctrico: Niveles altos de voltaje.
   Riesgos de incendio: Inflamabilidad de materiales.
   Riesgos de niveles inadecuados de energía eléctrica.
   Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
   Riesgos mecánicos: Inestabilidad de las piezas eléctricas.

Seguridad de la Información. Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación non-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

Seguridad Física: Consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y

alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Servidor: Computadora que ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes.

Sistema de Información.[16] Es un sistema que reúne, almacena, procesa y distribuye conjuntos de información entre los diferentes elementos que configuran una organización y entre la organización misma y su entorno.

Software: El software está compuesto por los programas que dirigen el funcionamiento de un ordenador. Es la "parte lógica" de la máquina que permite enlazar todos los elementos de hardware de la manera más efectiva posible, permitiéndole realizar cualquier tipo de trabajo.

Software malicioso: (malware) Es un término común que se utiliza al referirse a cualquier programa malicioso o inesperado o a códigos móviles como virus, troyanos, gusanos o programas de broma.

Terceros: Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema.

TI: Tecnología de la Información.

Usuarios: Se refiere a todos los empleados, proveedores, contratistas, o cualquier otra persona o entidad que por razón de su trabajo se le permita acceso, se le asignen derechos de uso y utilicen los recursos que componen los medios electrónicos de almacenamiento y transmisión de datos.

Virus: Son pequeños programas de computadora cuya principal cualidad es la de poder auto replicarse, está escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este para producir efectos dañinos.

Vulnerabilidades: Es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. Es decir, la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño. Están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño. Puede agrupar en grupos característicos: Ambiental, Física, Económica, Social, Educativa, Institucional y Política.

---

[16]PASTOR i. Collado, Joan Antoni. Concepto de Sistema de Informacion en la Organización. Universidad virtual. Editorial UOC. 2OO2.

2.4. MARCO TEÓRICO

2.4.1 Origen de la Norma ISO 27002.ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña[17].

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001
1992 Publicación BS 7750 - ahora ISO 14001
1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.
La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión

2.4.2 Normas de la serie ISO/IEC 27000.

ISO/IEC 27000: Fundamentos y vocabulario.
ISO/IEC 27001: Norma que especifica los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI).
ISO/IEC 27002 (actualmente ISO/IEC 17799-2005): Código de buenas prácticas para la gestión de Seguridad de la Información.

[17]ISO 27000. Origen de la norma ISO 27002. España. [en línea] Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO/IEC 27003: Directrices para la implementación de un sistema de gestión de Seguridad de la Información.
ISO/IEC 27004: Métricas para la gestión de Seguridad de la Información.
ISO/IEC 27005: Gestión de riesgos de la Seguridad de la Información.
ISO/IEC 27006: Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la Seguridad de la Información."

2.4.3 ISO 27002. Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. [18]

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.

Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

Dominios de la ISO 27002.[19]

Políticas de Seguridad
Aspectos Organizativos de la seguridad de la información
Gestión de activos
Seguridad ligada a los recursos humanos
Seguridad física y del entorno
Gestión de comunicaciones y operaciones
Control de acceso
Adquisición, desarrollo y mantenimiento de sistemas de información
Gestión de incidentes en la seguridad de la información
Gestión de la continuidad del negocio
Cumplimiento

2.5 MARCO LEGAL

2.5.1 Constitución Política de Colombia. Artículo 61[20]. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

[18]ISO 27000. ISO 27002. [en línea] Disponible en: http://www.iso27000.es/iso27000.html

[19]ISO 27000. Dominios de la ISO 27002:2013.[en línea] Disponible en: http://iso27000.es/download/ControlesISO27002-2013.pdf

[20]REPÚBLICA DE COLOMBIA, Constitución Política De La República De Colombia De 1991,Actualizada hasta el Decreto 2576 del 27 de Julio de 2005

2.5.2 Ley 1273 DE 2009[21]. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

El Congreso de Colombia

Decreta:

ARTÍCULO 1o. Adiciónese el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

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 1.000 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 1.000 salarios mínimos legales mensuales vigentes.

---

[21]Constitución política de Colombia. De la protección de la información y de los datos, Ley 1273 de 2009 [En Línea] Disponible en:
<http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm>

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 1.000 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 1.000 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.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II

De los atentados informáticos y otras infracciones

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 de este Código.

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 1.500 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.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

A fin de cumplir los objetivos propuestos para la realización del proyecto denominado "Formulación de controles basados en la norma NTC - ISO 27002 para la seguridad de la información en el Comité Departamental de Cafeteros del Cauca." fue necesario emplear un método de investigación descriptiva, que permitió formular hipótesis, para describir a grandes rasgos los aspectos aplicables a la investigación.

3.2 POBLACIÓN Y MUESTRA

3.2.1 Población Universo. En este proyecto el universo lo conformaron las 96 mil familias cafeteras vinculadas al Comité Departamental de Cafeteros del departamento del Cauca, con un total del 90% para las familias ubicadas en el área rural del Departamento. La población que se tuvo en cuenta la conformaron todos los empleados del Comité de Cafeteros seccional Popayán, alrededor de unas 73 personas distribuidas entre empleados de planta, aprendices y personal de apoyo.

3.2.2 Muestra. Una muestra es la parte que representa la población y reúne características que permiten la recolección de los datos relevantes. Para no perder la exactitud de la información se aplicóuna técnica de muestreo estadística, que representa con precisión a la población universo. Se requirió de 40 personas distribuidas entre empleados de planta, contratistas y aprendices para la muestra del proyecto.

3.3 TÉCNICAS DE INSTRUMENTACIÓN DE RECOLECCIÓN DE INFORMACIÓN

3.3.1 Técnicas de Recolección. Las técnicas e instrumentos de recolección que se emplearon para la recolección de la información necesaria en el desarrollo del proyecto fueron, la observación y la encuesta.

La encuesta es un cuestionario cuyas preguntas están enfocadas al problema y desarrollo del proyecto, esta técnica nos permitió tener en cuenta la opinión y requerimientos por parte de los usuarios finales y detectar fallasdel Comité de Cafeteros del Departamento del Cauca en la seguridad de la información. (Ver anexo A).

3.4 ANÁLISIS DE LA INFORMACIÓN

Para el análisis de la información fue necesario tomar como principal referencia los resultados de la encuesta, los cuales fueron tabulados y analizados detalladamente tomando muy en cuenta la opinión y el conocimiento de cada uno de los funcionarios que laboran en el Comité de Cafeteros.

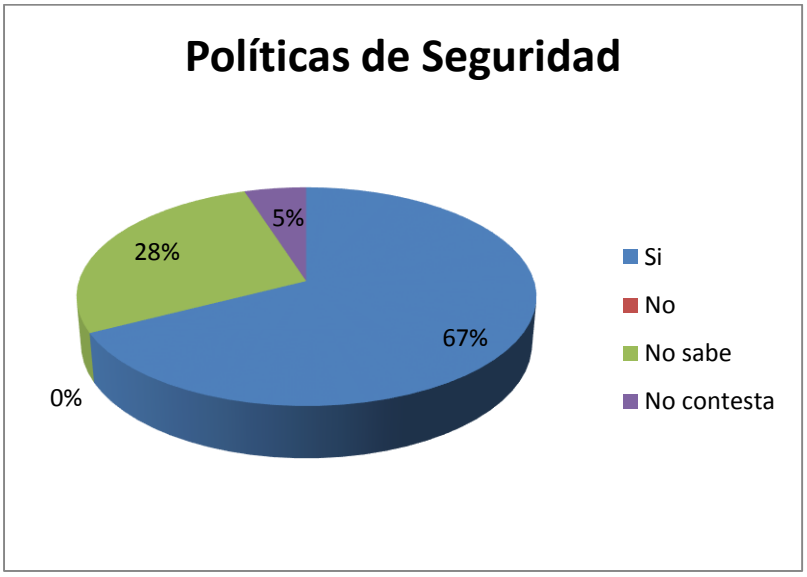
Los siguientes datos tabulados y graficados son los correspondientes a la encuesta realizada a 40 de los 73 trabajadores del Comité Departamental de Cafeteros del Cauca. (Ver Anexo1)

Tabla 1. El comité Departamental de Cafeteros del Cauca cuenta con políticas de seguridad de la información?

Alternativa	Cantidad	Porcentaje
Si	27	67
No	0	0
No sabe	11	28
No contesta	2	5

Fuente: Autor del proyecto de Investigación

Figura 1. Políticas de Seguridad



Fuente: Autor del proyecto de Investigación

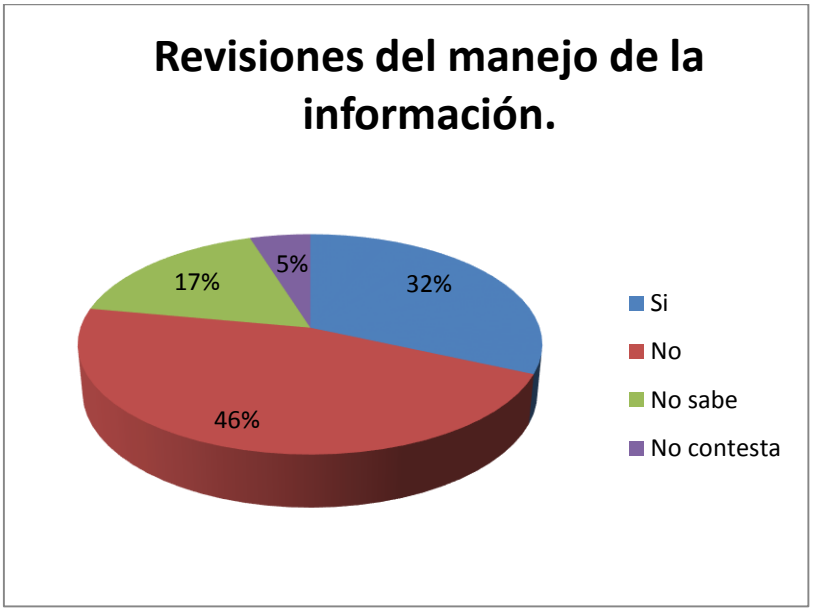
Según los resultados obtenidos en la figura 1, es necesario resaltar que la expectativa de la encuesta se basaba en poder garantizar un 100 % de conocimiento en cada una de las personas encuestadas, sobre la existencia de políticas de seguridad de la información en el Comité Departamental de Cafeteros del Departamento del Cauca. Se ratificó que un 67% es consciente del tema, sin embargo encontramos que un 28 % desconoce totalmente dicha información y un 5 % se abstiene de responder. Resulta conveniente de que el 33% de las personas que desconocen la política de seguridad de la información de la empresa, sean capacitadas en ello por parte del comité.

Tabla 2. En el comité realizan revisiones constantes a intervalos planificados en el manejo de la información para garantizar que ese manejo es adecuado, eficaz y suficiente?

Alternativa	Cantidad	Porcentaje
Si	13	32
No	19	46
No sabe	7	17
No contesta	2	5

Fuente: Autor del proyecto de Investigación

Figura 2. Revisiones del manejo de la información.



Fuente: Autor del proyecto de Investigación

La figura 2 muestra un déficit de un 46% que representa a todo aquel trabajador que aunque está bien informado sobre la política de seguridad de la información, manifiesta no conocer cuando se le realizan eventos de revisión a la información. Un 32 % es testigo de que se hace el debido proceso, un 17% concluye que no tiene conocimiento sobre el tema y un 5% sigue en abstinencia de responder. Que importante es que el comité genere un cronograma donde se dé a conocer varias actividades, entre las cuales este la revisión al manejo de la información de la empresa.

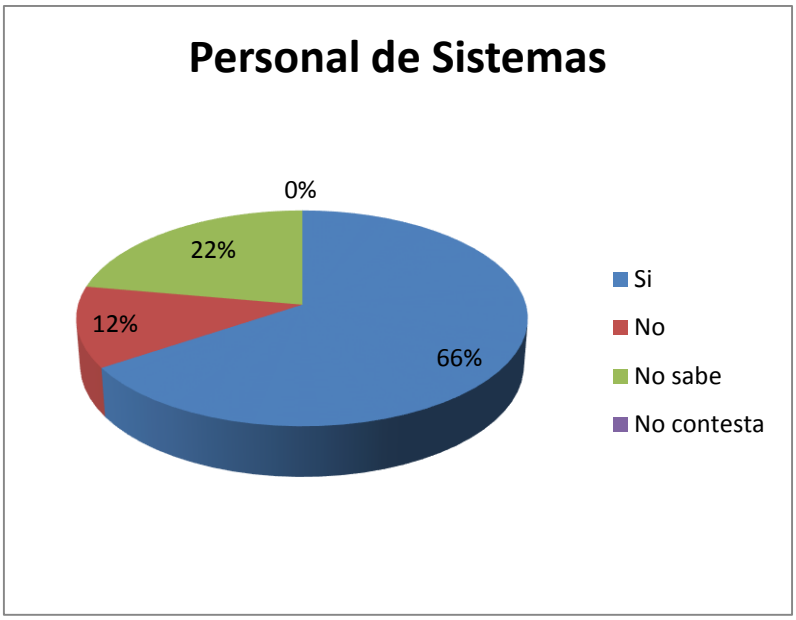
Tabla 3. La empresa cuenta con el personal idóneo en el área de sistemas?

Alternativa	Cantidad	Porcentaje

Si	26	65
No	5	13
No sabe	9	22
No contesta	0	0

Fuente: Autor del proyecto de Investigación

Figura 3. Personal de Sistemas



Fuente: Autor del proyecto de Investigación

El recurso humano es la herramienta fundamental de cada empresa, se hace indispensable contar con un personal capacitado para cumplir con cada labor de manera excelente. La figura 3 da un respaldo a este aspecto en un 66%, un 12% razona en que no es así y un 22% al parecer no sabe qué tipo de personal está dentro de la empresa. No se trata de desechar capital humano, sino de que el comité genere las herramientas de trabajo y capacite el personal, explotando al máximo sus capacidades con el fin generar un rendimiento óptimo dentro del área laboral.

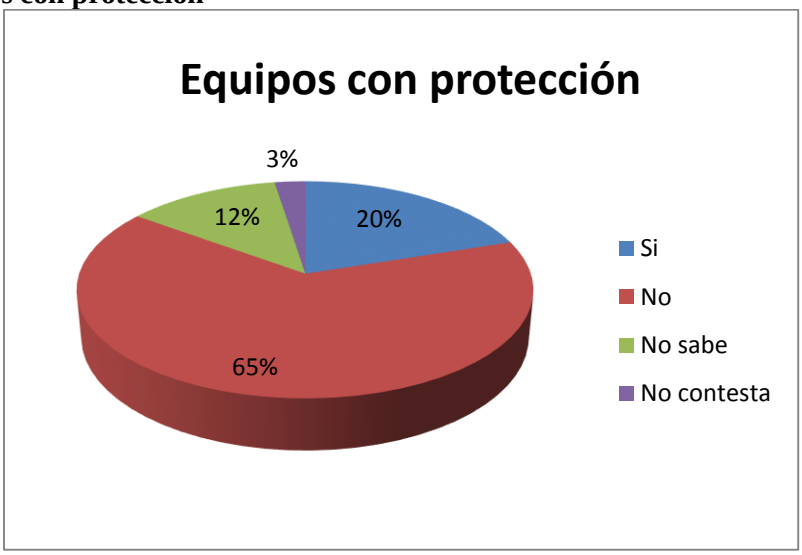
Tabla 4. Los equipos de sistemas cuentan con protección contra las amenazas físicas y ambientales?

Alternativa	Cantidad	Porcentaje
Si	8	20
No	26	65

No sabe	5	12
No contesta	1	3

Fuente: Autor del proyecto de Investigación

Figura 4. Equipos con protección



Fuente: Autor del proyecto de Investigación

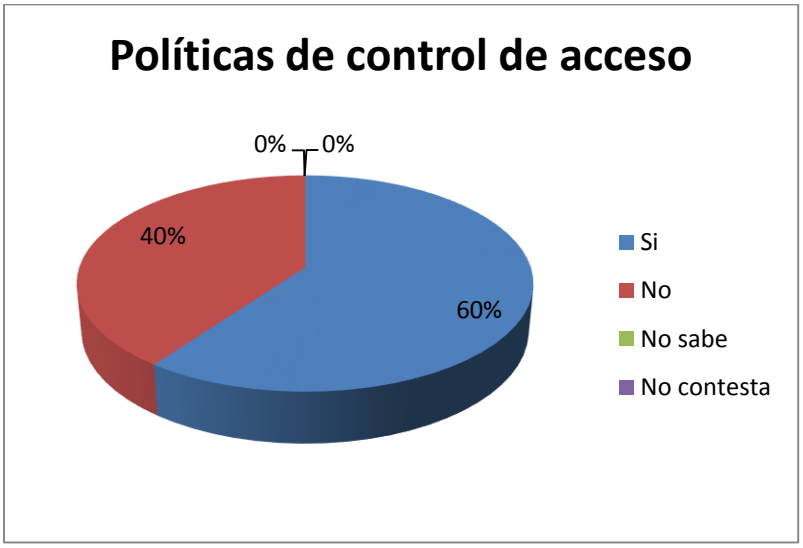
Un espacio agradable de trabajo requiere también del más mínimo detalle de seguridad. El comité debe generarle a su personal todas las herramientas necesarias que cuenten con las garantías de desarrollo laboral. Sin embargo en la figura 4 notamos claramente que un 65% no cuenta con protección en los equipos de trabajo, un 20% está satisfecho con su espacio laboral, un 12% todavía no sabe con qué protecciones cuenta y un 3% no responde.

Tabla 5. La organización tiene establecido políticas de control de acceso a diferentes dependencias especialmente la de sistemas?

Alternativa	Cantidad	Porcentaje
Si	24	60
No	16	40
No sabe	0	0
No contesta	0	0

Fuente: Autor del proyecto de Investigación

Figura 5. Políticas de control de acceso



Fuente: Autor del proyecto de Investigación

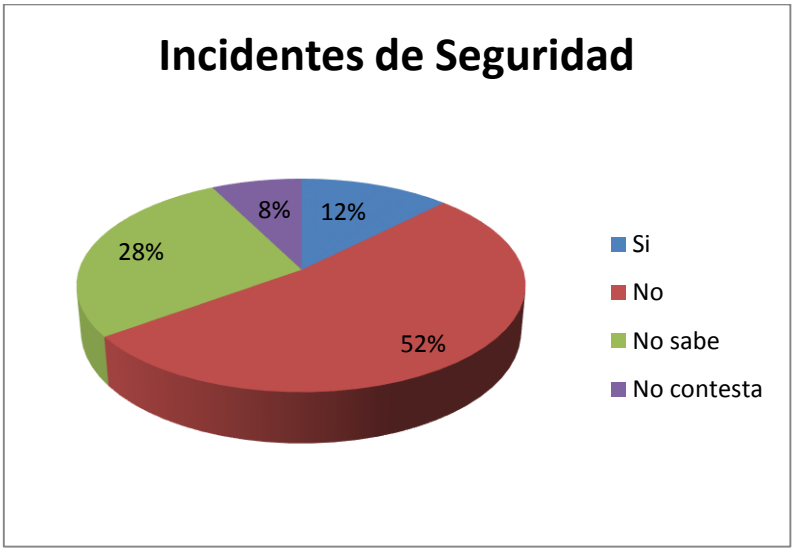
La figura 5 determina de que el 60% de los trabajadores encuestados está notificado de todas y cada una de las políticas de control de acceso a las dependencias de la empresa, mientras que el 40% opinan que no tienen clara estas políticas.

Tabla 6. La empresa reporta los Incidentes de Seguridad de la Información que se presenten?

Alternativa	Cantidad	Porcentaje
Si	5	12
No	21	52
No sabe	11	28
No contesta	3	8

Fuente: Autor del proyecto de Investigación

Figura 6. Incidentes de Seguridad



Fuente: Autor del proyecto de Investigación

Un incidente es algo que puede suceder en cualquier momento y es necesario saber cómo enfrentarlo y que cada uno de los trabajadores este en capacidad de solucionarlo cualquiera que sea. La figura 6 nos permite conocer que un 52% de los encuestados no saben cuándo se presenta un incidente, el 12% si es notificado, un 28% no sabe qué tipos de incidentes pueden ocurrir y el 8% no contesta

Después de tabular, graficar y analizar los resultados de la encuesta y teniendo en cuenta en gran instancia las entrevistas y las evidencias obtenidas de la observación realizada al Comité de Cafeteros se pudo concluir:
1.A pesar de que el Comité Departamental de Cafeteros del Cauca cuenta con políticas de seguridad de la información, la mayoría de sus empleados no tiene conocimiento de su existencia, también es importante resaltar que no se están realizando constantes revisiones al manejo de la información, por lo tanto no podemos garantizar que dicho manejo sea adecuado, eficaz y suficiente.

2. De cada una de las dependencias del Comité de Cafeteros, muchos de los equipos de cómputo cuentan con protección contra amenazas físicas y ambientales, no tienen un control de acceso establecido a cada área y especialmente no se cuenta con uno en el área de Sistemas. Además no se cuenta con una ruta de evacuación señalizada, no existen alarmas cercanas, ni se prohíbe el consumo de alimentos y bebidas o fumar y ninguna dependencia cuenta con aire acondicionado.

3. Sus empleados, no cuentan con acuerdos de confidencialidad de la información. Solo algunos realizan backup’s, memorias USB y Discos Duros personales, con una periodicidad semanal o mensual en el mejor de los casos.

4. En gran cantidad los equipos de cómputo del Comité de Cafeteros, tienen una contraseña de acceso pero no se hace un cambio periódico de esta, no cuentan con sistema operativo y software empresarial licenciado, mantienen restricciones de acceso a páginas web y en su mayoría cuentan con los requerimientos necesarios para que los empleados realicen sus labores diarias de manera óptima. No se le hace un mantenimiento constante a los equipos, más bien es realizado cuando lo requieran y solo el personal con más capacidades mantiene un antivirus actualizado.

4. PRESENTACION DE RESULTADOS

4.1 RECONOCIMIENTO DEL COMITÉ DEPARTAMENTAL DE CAFETEROS DEL CAUCA.

4.1.1 Direccionamiento Estratégico[22]

4.1.1.1 Misión. Asegurar el bienestar del caficultor colombiano a través de una efectiva organización gremial, democrática y representativa.

4.1.1.2 Visión. Consolidar el desarrollo productivo y social de la familia cafetera, garantizando la sostenibilidad de la caficultora y el posicionamiento del café de Colombia como el mejor del mundo.

4.1.1.3 Reseña Histórica. En 1927 los cafeteros colombianos se unieron con el fin de crear una organización que los representara nacional e internacionalmente, y que velara por su bienestar y el mejoramiento de su calidad de vida. Así nació la Federación Nacional de Cafeteros de Colombia (FNC), considerada hoy como una de las ONG rurales más grandes del mundo. La Federación es una entidad sin ánimo de lucro, y no está afiliada a ningún partido político.

La Federación Nacional de Cafeteros es la institución que representa a los caficultores colombianos. Sufortaleza principal radica en su carácter democrático y participativo. Es esta cualidad la que le permitepresentar legítimamente los intereses de todos los caficultores colombianos y ser su vocero ante elgobierno nacional y ante el mundo. Cada cuatro años, en el mes de septiembre, todos los cafeterosfederados con cédula cafetera eligen a sus representantes en un proceso democrático, como lo es el de laselecciones cafeteras.

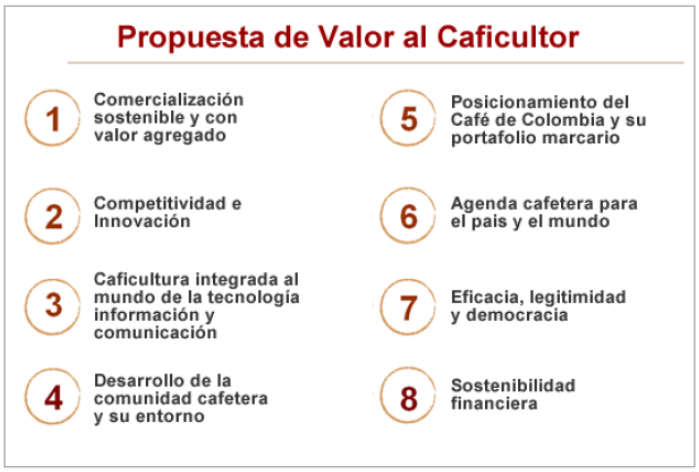
Existe un Comité Departamental de Cafeteros en cada una delas capitales de los departamentos cuya producción cafetera excede el dos por ciento (2%) del totalnacional. Funciona como órgano permanente integrado por seis (6) miembros principales con susrespectivos suplentes, los cuales son elegidos democráticamente en cada departamento en lascircunscripciones uninominales creadas para tal efecto; además, son los mismos delegados al CongresoCafetero. Entre sus principales funciones están la de organizar y orientar el gremio en el respectivodepartamento y la de ejecutar los distintos planes y programas para la región. El periodo de los miembros delComité será de cuatro años.

4.1.1.4 Objetivos. Orientar, organizar, fomentar y regular la caficultura colombiana procurando el bienestar del caficultor mediante mecanismos de colaboración, participación y fomento de carácter económico, científico, tecnológico, industrial y comercial, buscando mantener el carácter de capital social estratégico de la caficultora colombiana.

[22]FEDERACION NACIONAL DE CAFETEROS. Institucionalidad Cafetera (Noviembre de 2009).

4.1.1.5 Propuestas de Valor al Caficultor. Para garantizar la permanencia, sostenibilidad y futuro de la caficultura, se construyó a través del diálogo directo con el caficultor el Plan Estratégico 2008-2012, enfocado en ocho propuestas que le generarán valor al caficultor en forma integral, y le darán a la caficultura la capacidad de llegar con éxito a finales del siglo XXI.

Figura 7. Propuesta de Valor al Caficultor



Fuente:Comité Departamental de Cafeteros del Cauca. (Institucionalidad Cafetera)

Comercialización sostenible y con valor agregado:

Objetivos estratégicos:

Transferir el mejor precio posible al productor a través de la garantía de compra según el mercado internacional.
Continuar el ascenso en la cadena de valor.
Fomentar el consumo de café en el mercado interno.
Penetrar y consolidar nuevos mercados.
Ofrecer a clientes y consumidores un portafolio innovador que se adapte a sus necesidades.

Competitividad e Innovación:

Objetivos estratégicos:

Lograr una caficultura joven, productiva y rentable.
Incrementar la productividad del trabajo en la caficultura.
Garantizar la presencia institucional a través de una extensión rural innovadora y eficaz.
Proveer desarrollos científicos y tecnológicos oportunos y pertinentes.
Mejorar la calidad del café desde la finca.
Liderar iniciativas que generen un impacto positivo en el medio ambiente.

Caficultura integrada al mundo de la tecnología, información y comunicación:

Objetivos estratégicos:

Desarrollar e implementar esquemas virtuales de educación formal y capacitación.
Aprovechar los instrumentos tecnológicos para generar valor al caficultor y a la institucionalidad.
Acercar el cliente/ consumidor a la caficultura colombiana utilizando las herramientas tecnológicas y de información.

Desarrollo de la comunidad cafetera y su entorno:

Objetivos estratégicos:

Contribuir a mejorar los procesos educativos en la comunidad cafetera.
Apoyar e impulsar programas que mejoren las condiciones de salud y retiro de los caficultores.
Gestionar proyectos que mejoren la infraestructura de la comunidad.
Impulsar el desarrollo integral de la mujer cafetera.

Posicionamiento del Café de Colombia y su portafolio marcario:

Objetivos estratégicos:

Fortalecer la lealtad entre el cliente/ consumidor con el Café de Colombia y sus marcas asociadas.
Aumentar la penetración global del Programa 100% colombiano.
Fortalecer la imagen de "Juan Valdez" como símbolo de la calidad y los valores de los caficultores.
Avanzar en la diferenciación del café de Colombia como origen de calidad superior.

Agenda cafetera para el país y el mundo:

Objetivos estratégicos:

Representar a los caficultores colombianos en los diversos escenarios nacionales e internacionales.
Fortalecer la capacidad de la FNC como aliado para la política social y la inversión en el campo.
Apoyar al Estado en la consolidación de un modelo de equidad, desarrollo y paz para el sector rural Colombiano

Eficacia, legitimidad y democracia:

Objetivos estratégicos:

Fortalecer las competencias, el liderazgo y la comunicación gremial.
Asegurar la calidad del capital humano al interior de la organización.
Consolidar un modelo de administración innovador orientado al cliente y enfocado a resultados.
Optimizar la gestión del conocimiento.

Sostenibilidad financiera:

Objetivos estratégicos:

Fortalecer financieramente el FoNC, la FNC y sus entidades relacionadas.
Mantener las mejores prácticas en la administración financiera.
Optimizar la estructura de capital del FoNC y la FNC.

4.1.1.6 Estructura Orgánica del Comité Departamental de Cafeteros del Cauca. La Federación está conformada por los siguientes órganos y niveles jerárquicos:

Figura 8. Organigrama del Comité Departamental de Cafeteros del Cauca.

Fuente: Comité Departamental de Cafeteros del Cauca. (Institucionalidad Cafetera)

Congreso Nacional de Cafeteros: Es la máxima dirección de la Federación. Se reúne ordinariamente en Bogotá en el último bimestre de cada año. El Congreso está compuesto por los delegados de los departamentos, donde funcionan Comités Departamentales de Cafeteros, elegidos en seis circunscripciones uninominales que se constituirán para tal

efecto en cada uno de ellos. La elección del delegado de la respectiva circunscripción será efectuada por el voto directo de los cafeteros cedulados. Por cada delegado principal será elegido un suplente que lo reemplazará en su ausencia absoluta, temporal u ocasional.
Entre sus principales funciones están:

Considerar el informe de gestión anual elaborado por el gerente general y examinar las labores desarrolladas por la Federación en el año inmediatamente anterior.
Adoptar iniciativas que propendan por un mejor desempeño de las instituciones y organizaciones cafeteras.
Estudiar los problemas de la caficultura y dictar las medidas que se consideren adecuadas para su solución.
Elegir los miembros del Comité Directivo y los representantes gremiales al Comité Nacional, de conformidad con lo previsto en los estatutos.
Elegir el Gerente General de la Federación de una terna elaborada por el Comité Nacional de Cafeteros.

Comité Nacional de Cafeteros: Está conformado por los miembros acreditados por el Gobierno Nacional en virtud del contrato de administración del Fondo Nacional del Café, y por un representante de cada uno de los quince (15) comités departamentales de cafeteros, elegidos todos ellos por el Congreso Nacional de Cafeteros.

Los miembros del Comité actúan en beneficio de los agremiados de toda la nación y ejercen sus funciones procurando el bien común de los productores, de la actividad cafetera y de la economía nacional. Cada uno de ellos tiene, además, la condición de vocero especial de los caficultores de los departamentos según el renglón en que hubiere sido elegido y la obligación consiguiente de informar a los agremiados de los mismos sobre los temas de su gestión, recibir sus inquietudes y velar por sus intereses.
Entre sus principales funciones están:

Actuar como órgano de concertación de la política cafetera del país entre el gremio y el gobierno.
Orientar la política cafetera en las relaciones internacionales.
Cumplir las funciones y ejercer las atribuciones que les asignen los contratos que la Federación celebre o tenga celebrados con la nación y, en particular, las que se deriven de la administración y manejo del Fondo Nacional del Café.
Velar por el cumplimiento de las disposiciones legales que favorezcan a los productores y a la actividad cafetera, entendida como la producción y comercialización del grano y sus actividades accesorias y complementarias.
Adoptar y gestionar ante las entidades oficiales y privadas medidas eficaces que aseguren el desarrollo y defensa del bienestar de los productores y de la caficultura.

Comité Directivo: se encarga de la orientación de los asuntos gremiales y administrativos de la FNC. Delega en la Gerencia General y en los Comités Departamentales las funciones que considere convenientes. Está integrado por un representante de cada Comité Departamental de Cafeteros y cuenta con la asistencia del Gerente General.

Los actuales representantes del Comité Directivo son:

Juan Camilo Restrepo Salazar Comité de Cafeteros de Antioquia
Jorge Cala Robayo Comité de Cafeteros de Boyacá
Mario Gómez Estrada Comité de Cafeteros de Caldas
Fernando Castrillón Muñoz Comité de Cafeteros del Cauca
Crispín Villazón de Armas Comité de Cafeteros del Cesar – Guajira
Javier Bohórquez Bohórquez Comité de Cafeteros de Cundinamarca
Héctor Falla Puentes Comité de Cafeteros del Huila
Ramón Campo González Comité de Cafeteros de Magdalena
Hernán Román Calderón Comité de Cafeteros de Nariño
Alfredo Yánez Carvajal Comité de Cafeteros de Norte de Santander
Carlos Alberto Gómez Buendía Comité de Cafeteros de Quindío
Darío James Maya Hoyos Comité de Cafeteros de Risaralda
Jaime García Parra Comité de Cafeteros de Santander
César Eladio Campos Arana Comité de Cafeteros de Tolima
Carlos Roberto Ramírez Montoya Comité de Cafeteros del Valle

Entre sus principales funciones están:

Formular las políticas y adoptar las medidas necesarias para asegurar el desarrollo y la defensa de la caficultura y de su industria, y velar por su adecuado cumplimiento.
Considerar el plan estratégico preparado por la Gerencia General y efectuar el respectivo seguimiento.
Aprobar la estructura orgánica de la FNC.
Reglamentar las decisiones del Congreso Nacional de Cafeteros y hacer que se pongan en ejecución.
Estudiar el proyecto de presupuesto del Fondo Nacional del Café y la Federación preparado por la Gerencia General y autorizar su presentación al Congreso Nacional.

Comités Departamentales de Cafeteros: existe un Comité Departamental de Cafeteros en cada una de las capitales de los departamentos cuya producción cafetera excede el dos por ciento (2%) del total nacional. Funciona como órgano permanente integrado por seis (6) miembros principales con sus respectivos suplentes, los cuales son elegidos democráticamente en cada departamento en las circunscripciones uninominales creadas para tal efecto; además, son los mismos delegados al Congreso Cafetero.

Entre sus principales funciones están la de organizar y orientar el gremio en el respectivo departamento y la de ejecutar los distintos planes y programas para la región. El periodo de los miembros del Comité será de cuatro años.

Los Comités Departamentales de Cafeteros tienen las siguientes funciones:
Organizar y promover el Gremio en el departamento y hacer lo propio con los Comités Municipales.

Promover el desarrollo de cooperativas de caficultores, siguiendo para ello las políticas que fijen los Congresos Nacionales de Cafeteros, el Comité Directivo y la Gerencia General.
Aprobar su planta de cargos, en concordancia con las políticas y directrices impartidas por la Gerencia General y el Comité Directivo, la cual deberá someterse para su consideración y aprobación.
Nombrar a su Director Ejecutivo y removerlo, por iniciativa propia o a solicitud del Gerente General, cuando existan serios motivos para ello, originados en actuaciones que menoscaben el buen nombre de la Federación, atenten contra su patrimonio, violen los estatutos o sus reglamentos.
Cumplir y hacer cumplir los estatutos, las instrucciones del Congreso Nacional de Cafeteros, del Comité Nacional de Cafeteros, del Comité Directivo y de la Gerencia General, y velar por el cumplimiento de los reglamentos en los respectivos departamentos.
Vigilar el manejo de los fondos que le correspondan.
Atender las consultas de los Comités Municipales y practicar visitas a estos.
Elaborar, en coordinación con el Director Ejecutivo, el proyecto de presupuesto, de acuerdo con lo establecido por el Comité Nacional de Cafeteros, por el Comité
Directivo y por la Gerencia General, según el caso, y someterlo a la aprobación correspondiente.
Velar por la correcta y oportuna prestación de los servicios del Gremio a los caficultores, por parte de las dependencias de la Federación, o de las compañías vinculadas a ella que operen en el departamento.
Enviar copia íntegra de las actas de sus sesiones a la Gerencia General y mantener informados a los Comités Municipales de su jurisdicción acerca de las decisiones que adopten.
Colaborar con los Comités Municipales en el fomento de las industrias complementarias del café. Autorizar la condonación de faltantes o glosas a cargo de empleados o contratistas suyos, dentro de los límites y cuantías que el Comité Directivo señale, sin perjuicio de las investigaciones a que haya lugar.
Aplicar la política salarial de sus empleados en concordancia con las políticas salariales y las pautas presupuestales determinadas por el Comité Directivo y la Gerencia General.
Dirimir los empates que se hayan presentado en los Comités Municipales de cafeteros y que subsistan luego de tres (3) votaciones.
Orientar los servicios de extensión y de educación, con sujeción a las políticas generales dictadas por el Comité Directivo.
Ejecutar, por conducto de su Director Ejecutivo, las distintas campañas ordenadas por iniciativa propia o de la Gerencia General, con sujeción a las políticas generales trazadas por el Congreso Nacional de Cafeteros, el Comité Nacional y el Comité Directivo.
Gestionar, con las entidades locales y el gobierno departamental, obras, programas y acciones que beneficien a los caficultores de la región.

Comités Municipales de Cafeteros: funcionan en aquellos municipios donde existen al menos 400 cafeteros cedulados y su producción anual sea igual o superior a 60.000 arrobas. Están compuestos por seis miembros principales con sus respectivos suplentes personales elegidos por los productores federados. Se encargan de la organización y representación de los caficultores del municipio y actúan como voceros ante el respectivo Comité Departamental.

Las funciones del Comité Municipal son:

Cumplir y hacer cumplir los estatutos y las políticas del Congreso Nacional de Cafeteros, así como las decisiones del Comité Directivo, de la Gerencia General y de los Comités Departamentales.

Adelantar, en coordinación con el Comité Departamental, campañas para el mejoramiento del cultivo, el control de plagas y enfermedades, la renovación de los cafetales, el correcto beneficio del café y todas las que redunden en el mejoramiento de las condiciones sociales y económicas de los productores de café.

Servir de voceros de los productores de café para las solicitudes que estos deseen hacer a los Comités Departamentales, o por su conducto, al Comité Directivo en aquellos departamentos donde no exista el Comité Departamental, con el fin de obtener soluciones que favorezcan la organización, defensa y desarrollo de la caficultura, y en especial, las que pongan remedio a las dificultades y problemas que en cada municipio ella confronte.

Promover la cedulación cafetera de los productores de café y divulgar los derechos, deberes, servicios y beneficios que corresponden a los miembros de la Federación.

Procurar que en el respectivo municipio se cumplan las leyes y decretos o disposiciones tendientes a mantener la sanidad vegetal y el medio ambiente, y todas aquellas disposiciones que beneficien a los caficultores. Solicitar el apoyo del Comité Departamental cuando se considere conveniente.

Cooperar para el buen éxito de las campañas que en sus municipios adelante el Comité Departamental, para lo cual harán oportunamente las sugerencias que estimen convenientes.

Estudiar y resolver las solicitudes de los cafeteros del respectivo municipio o, si fuere el caso, enviarlas acompañadas de su concepto al respectivo Comité Departamental o a las entidades públicas o privadas competentes para decidir.

Colaborar con las juntas de acción comunal, con las entidades gremiales y con los empleados de la Federación en el establecimiento de las metas de trabajo y el programa de desarrollo de sus comunidades.

Elaborar los planes indicativos de obras e inversiones en sus jurisdicciones, establecerles prioridades y someterlos a la aprobación del respectivo Comité Departamental. Para estos efectos, Dicho Comité pondrá a disposición del Comité Municipal sus recursos técnicos y logísticos. Si no existe Comité Departamental, los planes indicativos de obras e inversiones se someterán a la aprobación de la Gerencia General de la Federación Nacional de Cafeteros.

Gestionar con entidades locales y el gobierno municipal programas y acciones que beneficien a los caficultores de la región.

4.1.1.7 Organización por procesos

Figura 9. Procesos Cafeteros

Fuente: Comité Departamental de Cafeteros del Cauca (Institucionalidad Cafetera)

Procesos dentro de la organización

- **Investigación**
  Objetivo: generar tecnologías y conocimientos apropiados, competitivos y sostenibles, para mejorar la producción de café y así contribuir al bienestar de los caficultores colombianos
- **Extensión rural**
  Objetivo: educar mediante procesos tecnológicos, sociales, culturales, económicos y gremiales, para lograr el cambio de actitud en el caficultor, de tal forma que genere bienestar para él, su familia y la comunidad.

- **Fortalecimiento gremial**
  Objetivo: lograr la participación activa y fortalecer el sentido de pertenencia de cada uno de los productores federados en la Federación Nacional de Cafeteros de Colombia.

- **Gestión de proyectos de desarrollo social**
  Objetivo: estructurar proyectos de desarrollo social, con el fin de mejorar las condiciones de vida del caficultor y la comunidad en las zonas cafeteras.

- **Regulación de la política cafetera**
  Objetivo: asegurar la competitividad del café colombiano, integrando a todas las partes relacionadas en la comercialización, mediante el establecimiento, divulgación

y ejecución de normas y políticas relacionadas con calidad, transformación y exportación de café.

- **Gestión de mercadeo e innovación**
  Objetivo: analizar las diferentes variables del mercado para diseñar productos acordes con las necesidades y expectativas del cliente.

- **Compras y logística de aprovisionamiento**
  Objetivo: negociar el precio y otras condiciones de compra de acuerdo con los requerimientos establecidos en la planeación teniendo en cuenta la garantía de compra.

- **Ventas**
  Objetivo: realizar la negociación y formalizar el precio correspondiente en el menor tiempo posible.

- **Transformación y logística de distribución**
  Objetivo: agregar valor a la materia prima para la obtención de los productos de venta y coordinar las actividades de distribución cumpliendo con los requerimientos del cliente al menor costo posible.

- **Servicio al cliente**
  Objetivo: lograr lealtad en los clientes a través de una respuesta oportuna y efectiva a sus inquietudes o iniciativas basados en un flujo de comunicación eficiente.

- **Procesos de apoyo administrativo y financiero**
  Objetivo: apoyar las unidades estratégicas de negocio a través de la consolidación y prestación de los servicios que las soportan, con la más alta calidad posible, optimizando los costos e incrementando la productividad.

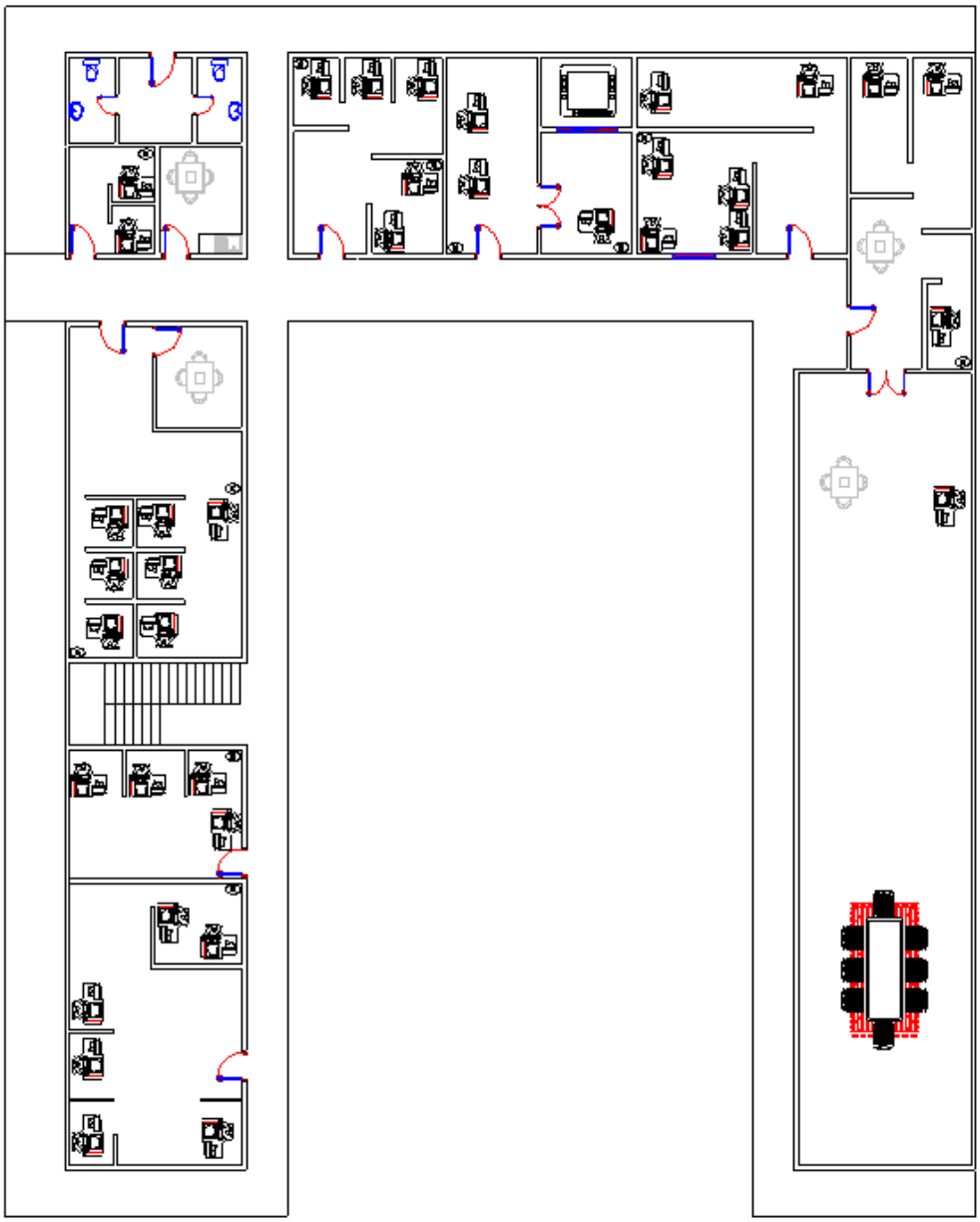
- **Propiedad intelectual**
  Objetivo: asegurar los intangibles (marcas, secretos de empresa, derechos de autor y tecnología) del FoNC y la FNC, a través de políticas que rijan su manejo y permitan el aprovechamiento estratégico y comercial de los mismos.

4.1.1.8 Planos de la Organización.

Figura 10. Plano – Primer Piso

Fuente. Autor del Proyecto de Investigación

Figura 11. Plano – Segundo Piso



Fuente. Autor del Proyecto de Investigación

4.2 ANALISIS DE LA NORMA ISO/IEC 27002

ISO / IEC 27002 es una norma internacional que establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización.[23]

ISO/IEC 27002 tiene como objetivos los siguientes puntos:

Servir de punto de información de la serie de normas ISO 27000 y de la gestión de seguridad de la información mediante la aplicación de controles óptimos a las necesidades de las organizaciones en cada momento.
Realizar la libre difusión de información en español en base a las investigaciones, conocimientos y búsquedas de los editores de la web.
Responder a todas las consultas recibidas en relación a las normas de la serie ISO 27000, independientemente de su origen (empresas grandes, Pymes, organismos públicos, estudiantes, etc.Establecer contactos con todo tipo de organizaciones, desarrolladores y personas relacionadas con la norma, con el objetivo de intercambiar informaciones, opiniones, experiencias o conocimientos, e impulsar la colaboración en actividades de fomento y promoción de las buenas prácticas para la aplicación de controles para la seguridad de la información.

Tabla 7. Características de la ISO 27002

ISO 27002	
Significado de las Siglas:	Organización Internacional de Normalización y Comisión Electrotécnica Internacional.
Creado por:	La Organización Internacional de Normalización (ISO) y Comisión Electrotécnica Internacional (IEC).
Carácter de Fundamentación:	Marco de Mejores Prácticas. Es un anexo del Estándar 27001 para la seguridad de la información.
Definición:	Es un estándar de seguridad que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.
Estructura	Está compuesta por 39 objetivos de control y 133 controles, agrupados en 11 dominios para seguridad de la información.

[23]AYALA. Eric A. Familia de Normas. Universidad tecnológica de panamá. Panamá. [en línea]. http://www.academia.edu/8525804/NORMA_ISO_27001

Características:	- Es la única norma que no sólo cubre la problemática de la seguridad TI sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja. - En distintos ámbitos, permite conocer qué se puede hacer para mejorar la seguridad de la información. - Expone, en distintos campos, una serie de apartados a tratar en relación a la seguridad, los objetivos de seguridad a perseguir, una serie de consideraciones (controles) a tener en cuenta para cada objetivo y un conjunto de "sugerencias" para cada uno de esos controles. - Facilita la integración de los sistemas de gestión, debido a que es una estructura de alto nivel, donde los términos y definiciones ayudan a implementar.
Funciones y Orientación	Marco de referencia de seguridad de la información.
Permite:	- Flexibilidad de controles para su uso en la forma en que una organización quiere protegerse a sí mismo. - Aumentar la reputación de los negocios que han implementado la norma. - Proteger a las empresas mediante la identificación de riesgos y estableciendo controles para gestionarlos o reducirlos. - Ayudar a los grupos de interés y aumentar la confianza del cliente, teniendo sus datos protegidos. - Aumentar las oportunidades de acceso a licitaciones mediante la demostración de cumplimiento y obtener un estatus como proveedor preferido.
Beneficios:	- Reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. - Reducción de las amenazas hasta alcanzar un nivel asumible para la organización. - En caso de producirse una incidencia, los daños se minimizan y la continuidad del negocio está asegurada. - Ahorro de costes derivado de una racionalización de los recursos. - Eliminación de las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos. - Se Considera a la seguridad como un sistema, y esta se convierte en una actividad de gestión. - La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la organización. - Se asegura a la organización del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. - La entidad se asegura del cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.
Para que se Implementa:	Cumplimiento del estándar de seguridad de la información.
Quiénes lo	Compañías de consultoría en TI, Empresas de seguridad de información y

Evalúan:	consultores de seguridad en redes.
Ventajas:	A la organización: - Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial. - Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación. Al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial: - Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información. - Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información. - Al realizar procesos de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora. - Aumento de la seguridad efectiva de los sistemas de información - Correcta planificación y gestión de la seguridad de la información. - Garantías de continuidad del negocio. - Mejora continua a través del proceso de auditoría interna. - Incremento de los niveles de confianza de los clientes. - Aumento del valor comercial y mejora de la imagen de la organización.
Desventajas**:**	- Al iniciar este conjunto de tareas, no cabe duda que se está sobrecargando el ritmo habitual de trabajo de toda la organización, por lo tanto se debe ser consciente de que exigirá un esfuerzo adicional. -Independientemente de las tareas periódicas que implica, una vez lanzado el SGSI para los administradores del mismo, el mantenimiento del nivel alcanzado, requerirá inexorablemente un esfuerzo continuado de toda la organización al completo. - Sea cual fuere la elección, el cúmulo de actividades realizadas exige un mantenimiento y mejora continua, sino deja de ser un SGSI, y ello salta a la vista en el muy corto plazo. Es decir no se puede dejar de lado, pues al abandonar un cierto tiempo el SGSI, requerirá un esfuerzo similar a lanzarlo de nuevo. - La implantación de ISO/IEC 27002 en una organización, es un proyecto que suele tener una duración entre seis y doce meses, dependiendo del grado de madurez en seguridad de la información. - Es recomendable la ayuda de consultores externos. - El equipo de proyectos de implantación, debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI.
Metas o Alcances:	- Establecer los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. - Proporcionar un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados. - Ser implementada para satisfacer los requerimientos identificados por una evaluación del riesgo.

	- Servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas. - Ayudar a elaborar la confianza en las actividades inter-organizacionales.
Utilización:	Legislativo. - Protección de datos y privacidad de la información personal. - Protección de los registros organizacionales. - Derechos de propiedad intelectual.
A Quién está Dirigida:	- A oficiales de seguridad de la información. - A oficiales del cumplimiento. - A oficiales de la privacidad de datos. - Auditores internos. - A auditores que quieran liderar auditorías de certificación de Sistema de Gestión de Seguridad de la información (SGSI). - Agerentes de proyectos o consultores que quieren dominar los procesos de auditoría de Sistemas de Gestión de Seguridad de la Información (SGSI). - A altos directivos responsables de la dirección de una empresa y la gestión de sus riesgos. - A Miembros de un equipo de seguridad de la información. - A Instructores en seguridad de la información.
Herramientas Utilizadas:	-Intercambio y movilidad (Red externa y red local). -Soportes físicos. -Servicios externos. -Seguridad física. -Desarrollo y Mantenimiento (Documentación, servidores, aplicaciones y puestos de trabajo). -Organización. -Usuarios.
Confiabilidad:	Alta

Fuente: Adaptado de SANCHEZ A. Kathedrin. Diseño de las políticas de seguridad de la información para la alcaldía municipal de Río de Oro, Cesar. UFPSO

Tabla 8. Cláusulas ISO 27002:2013

Cláusulas de la ISO 27002.

#	Dominios	Objetivos de control
0	Introducción	
1	Campo de Aplicación	
2	Términos y definiciones	
3	Estructura del estándar	
4	Evaluación y tratamiento del riesgo	
5	Política de seguridad de la información	**5.1.** Directrices de la dirección en la seguridad de la información.
6	Aspectos Organizativos de la seguridad de la información	**6.1.** Organización interna. **6.2.** Dispositivos para movilidad del teletrabajo
7	Recursos Humanos	**7.1.** Antes de la contratación **7.2.** Durante la contratación **7.3**. Cese o cambio de puesto de trabajo
8	Gestión de Activos	**8.1.** Responsabilidad sobre los activos **8.2.** Clasificación de la información **8.3.** Manejo de los soportes de almacenamiento
9	Control de accesos	**9.1.** Requisitos de Negocio para el control de acceso. **9.2.** Gestión de acceso del usuario. **9.3.** Responsabilidades del usuario. **9.4**. Control de acceso a sistemas y aplicaciones
10	Cifrado	**10.1.** Controles criptográficos
11	Seguridad física y ambiental	**11.1.** Áreas Seguras **11.2.** Seguridad de los equipos
12	Seguridad en la operativa	**12.1.** Responsabilidades y procedimientos de operación. **12.2.** Protección contra código malicioso. **12.3.** Copias de seguridad. **12.4.** Registro de actividad y supervisión **12.5.** Control de software en explotación **12.6.** Gestión de vulnerabilidad técnica **12.7.** Consideraciones de las auditorias de los sistemas de información
13	Seguridad en las telecomunicaciones	**13.1.** Gestión de la seguridad de redes. **13.2.** Intercambio de información con partes externas.
14	Adquisición, desarrollo y mantenimiento de sistemas de	**14.1.** Requisitos de seguridad de los sistemas de información

	información	**14.2.** Seguridad de los procesos de desarrollo y soporte **14.3.** Datos de prueba
15	Relaciones con suministradores	**15.1.** Seguridad de la información en las relaciones con suministradores **15.2.** Gestión de prestación de servicio por suministradores
16	Gestión de Incidentes de Seguridad de la información	**16.1**. Gestión de incidentes de seguridad de la información y mejoras
17	Aspectos de seguridad de la información en la gestión de continuidad del negocio	**17.1.** Continuidad de la seguridad de la información **17.2.** Redundancias
18	Cumplimiento	**18.1.** Cumplimiento de los requisitos legales y contractuales **18.2.** Revisiones de la seguridad de la información.

Fuente: Autor del proyecto de Investigación

En total laISO/IEC 27002 contiene 11 cláusulas de control de seguridad.

A continuación se detallan las diferentes cláusulas con sus categorías y los objetivos que persiguen cada una de ellas[24]

0. **Introducción:**

   Conceptos generales de seguridad de la información y SGSI.

1. **Campo de aplicación**

   Se especifica el objetivo de la norma.

2. **Términos y definiciones**

   Es una breve descripción de los términos más usados en la norma.

3. **Estructura del estándar**

   Descripción de la estructura de la norma.

4. **Evaluación y tratamiento del riesgo**

[24]ISO 27002. Clausulas.[en línea]. Disponible en: http://www.iso27002.es/

Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

5. **Política de Seguridad**

   Política de seguridad de la información. Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes.

6. **Aspectos organizativos de la Seguridad de la Información**

   Organización interna. Gestionar la seguridad de la información dentro de la Organización.

   Terceros. Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros.

7. **Seguridad ligada a los Recursos Humanos**

   Seguridad de la definición del trabajo y los recursos. Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

   Seguridad en el desempeño de las funciones del empleo. Asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos.

   Finalización o cambio del puesto de trabajo. Garantizar que los empleados, contratistas y terceras personas abandonan la organización o cambian de empleo de forma organizada.

8. **Gestión de Activos**

   Responsabilidad sobre los activos. Alcanzar y mantener una protección adecuada de los activos de la Organización

   Clasificación de la información. Asegurar que se aplica un nivel de protección adecuado a la información.

9. **Control de Acceso**

Requerimiento de negocio para el control del acceso. Controlar los accesos a la información.

Gestión de acceso de usuario. Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

Responsabilidades de usuario. Impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.

Control de acceso en red. Impedir el acceso no autorizado a los servicios en red.

Control del acceso al sistema operativo. Impedir el acceso no autorizado al sistema operativo de los sistemas.

Control de acceso a las aplicaciones. Impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.

Información móvil y tele-trabajo. Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.

10. Cifrado

Controles criptográficos. Proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.

11. Seguridad Física y del entorno

Áreas seguras. Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.

Seguridad de los equipos. Evitar la pérdida, daño, robo o puesta en peligro de los activos y interrupción de las actividades de la organización

12. Seguridad en la operativa

Procedimientos y responsabilidades de operación. Asegurar la operación correcta y segura de los recursos de tratamiento de información.

Protección contra software malicioso y código móvil. Proteger la integridad del software y la información.

Gestión interna de soporte y recuperación. Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

Supervisión de los servicios contratados a terceros. Implementar y mantener un nivel apropiado de seguridad de la información y de la prestación del servicio en línea con los acuerdos de prestación del servicio por terceros.

Servicios de comercio electrónico. Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.

Utilización y seguridad de los soportes de la información. Evitar la divulgación, modificación, retirada o destrucción de activos no autorizada e interrupciones en las actividades de la organización.

Monitorización. Detectar actividades de procesamiento de la información no autorizadas

13. Seguridad en las telecomunicaciones.

Gestión de redes. Asegurar la protección de la información en las redes y la protección de su infraestructura de apoyo

Intercambio de información y software. Mantener la seguridad de la información y del software que se intercambian dentro de la organización o con cualquier entidad externa.

14. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Requerimientos de seguridad de los sistemas. Garantizar que la seguridad es parte integral de los sistemas de información.

Seguridad en los procesos de desarrollo y soporte. Mantener la seguridad del software del sistema de aplicaciones y la información.

Seguridad de los ficheros del sistema. Garantizar la seguridad de los sistemas de ficheros.

Gestión de la Vulnerabilidades Técnicas. Reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas.

15. Relaciones con suministradores

Seguridad de la información en las relaciones con los suministradores. Evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información.

16. Gestión de Incidentes de Seguridad de la Información

Comunicación de eventos y debilidades de la seguridad de la información. Garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.

Gestión de los incidentes y mejoras en la seguridad de la información. Garantizar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de información.

17. Gestión de la Continuidad del Negocio

Aspectos de la gestión de la continuidad del negocio. Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.

18. Cumplimiento

Cumplimiento de los requerimientos legales. Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.

Revisiones de la política de seguridad, y cumplimiento técnico. Garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la Organización.

Consideraciones sobre la auditoría de sistemas. Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde éste proceso.

Para el desarrollo de este trabajo y analizando los hallazgos encontrados en el comité departamental de cafeteros del cauca se seleccionó la norma ***ISO/IEC 27002***, ya que es un marco de trabajo de mejores prácticas internacionales que establece las guías y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en el comité departamental de cafeteros del cauca.Sus objetivos de control y controles son recomendados para cubrir los requerimientos de seguridad que han surgido luego de una evaluación de riesgos.

4.3HALLAZGOS ENCONTRADOS EN EL COMITÉ DEPARTAMENTAL DE CAFETEROS DEL CAUCA.

A continuación se muestran los hallazgos encontrados en el Comité Departamental de Cafeteros del Cauca, una breve descripción de cada uno de ellos y la aplicación de los controles de la ISO 27002 adecuados, para contrarrestar las debilidades y amenazas que se presentan respecto a la seguridad de la información.

Tabla 9. Hallazgos

HALLAZGOS	DESCRIPCION	CONTROL ISO 27002:2013
En gran cantidad los equipos de cómputo del Comité de Cafeteros, tienen una contraseña de acceso pero no se hace un cambio periódico.	Las contraseñas de acceso a los equipos de cómputo, correos electrónicos, sistemas de información SICA, no son cambiadas periódicamente, siempre manejan la misma contraseña.	**9. CONTROL DE ACCESOS.** 9.2.2 Gestión de los derechos de acceso asignados a usuarios Se debería asegurar el acceso de usuarios autorizados a fin de prevenir el acceso no autorizado a los sistemas y servicios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. Se debería restringir y controlar la asignación y uso de los privilegios de usuario en cada equipo de computo
A pesar de que el Comité de Cafeteros cuenta con cableado estructurado, este se queda corto para la cantidad de equipos que están en red.	El exceso de equipos en las oficinas hace que los nodos se agoten	**SEGURIDAD EN LAS TELECOMUNICACIONES** 13.1.1 Controles de red. Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.
No se realizan mantenimientos preventivos y correctivos periódicamente a los equipos de cómputo.	En la cooperativa no se hacen mantenimientos preventivos periódicamente tanto de hardware como de software, los antivirus instalados en los equipos de cómputos se encuentran desactualizados en algunas áreas.	**11. SEGURIDAD FISICA Y AMBIENTAL** 11.2.4 Mantenimiento de los equipos. Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. **12. SEGURIDAD EN LA OPERATIVA** 12.2.1 Protección contra código malicioso.

		Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.
No se le da el correcto proceso al manejo de las copias de seguridad realizadas por la empresa. Solo algunos empelados realizan backup's en memorias USB y Discos Duros personales, con una periodicidad semanal o mensual en el mejor de los casos.	Inadecuado manejo de las copias de seguridad, que han hecho que en la entidad ya se hayan presentado situaciones preocupantes de pérdida de información, sin consecuencias graves hasta ahora, pero duplicando el trabajo mientras se recupera dicha información y con una alta posibilidad de que sigan ocurriendo estos incidentes, que más adelante si podrían dejar secuelas de mayor envergadura.	**12 SEGURIDAD EN LA OPERATIVA** **12.3.1**Copias de seguridad de la información. Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación.
No se evidencia un plan de contingencia visible para los funcionarios que hacen parte del comité de cafeteros.	El Comité Departamental de Cafeteros del Cauca en la actualidad no cuenta con un plan de contingencia que respalden o contengan técnicas humanas y organizativas necesarias para garantizar la continuidad y las operaciones del área.	**11. SEGURIDAD FISICA Y AMBIENTAL** 11.1.4 Protección contra las amenazas externas y de origen ambiental. Se debe designar y aplicar medidas de protección física contra incendios, inundación, terremoto, explosión, malestar civil y otra forma de desastre natural o humano.
El inventario de hardware y software no se encuentran actualizados.	No se cuenta con un formato o registro actualizado que evidencie el inventario de hardware que posee el comité, por tal motivo se desconoce la ubicación exacta de dichos elementos como son equipos de cómputo, impresoras entre otros.	**GESTION DE ACTIVOS** 8.1.1 Inventario de Activos Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes. 8.1.2 Propiedad de los activos Toda la información y activos asociados a los

		recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
Algunos funcionarios instalan software descargados de internet no licenciado sin ninguna restricción de la empresa.	Como no existe restricción en las descargas de internet, algunos empleados instalan software gratuitos sin dejar registros de los acuerdos de instalación que contiene de dicho software.	**9. CONTROL DE ACCESO** 9.2.3 Gestión de privilegios. Se debería restringir y controlar la asignación y uso de los privilegios. **11 SEGURIDAD FISICA Y AMBIENTAL** 11.2.9. Políticas de puesto de trabajo despejado y pantalla limpia. Políticas para escritorios y monitores limpios de información.
Los extintores no se encuentran en un área útil y no tienen la fecha de recarga vencida para su uso.	Los extintores no están ubicados en los lugares que se necesiten y tampoco contienen las fechas de recargas actualizadas que evite problemas en el momento de utilizarlos.	**11. SEGURIDAD FÍSICA Y DEL ENTORNO** 11.1.3 seguridad de las oficinas, despachos e instalaciones. Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y de origen ambiental. Se debe designar y aplicar medidas de protección física contra incendios, inundación, terremoto, explosión, malestar civil y otra forma de desastre natural o humano.
El comité de cafeteros cuenta con políticas de seguridad de la información pero la mayoría de sus empleados no tiene conocimiento de su existencia, por ende no las aplican.	Existen políticas de seguridad de la información pero muchos de los empleados no las conocen por tal razón,cualquier empleado puede estar violando la seguridad sin conocimiento alguno.	**POLITICAS DE SEGURIDAD** 5.1.1 Documento de política de seguridad de la información. La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los

		empleados y las partes externas relevantes. **SEGURIDAD LIGADA A LOS RECURSOS HUMANOS** 7.2.2 Capacitación, educación y concientización en seguridad información Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.
No se tienen establecidos mecanismos de autenticación de usuarios a la red interna del comité de cafeteros.	En la realización de la lista de chequeo se evidencio por parte de un funcionario que no se cuenta con acceso remoto a la red. Los funcionarios del Comité, tienen acceso a la información desde lugares ajenos a la entidad.	**CONTROL DE ACCESO** 11.4.2 Autenticación de usuario para conexiones externas. Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios.
No llevan un control de entrada a las áreas seguras, como oficinas.	Actualmente no se cuenta con un registro y control de entrada a oficinas, dependenciasy/o áreas de mayor seguridad del Comité de Cafeteros, además el acceso especial al área de sistemas y telecomunicaciones no tiene ninguna restricción.	**11 SEGURIDAD FISICA Y AMBIENTAL** 11.1.2 Controles físicos de entrada. Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado 11.1.3 Seguridad de oficinas, despachos y recursos. Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.

No se encuentra señalizada las rutas de evacuación, no existen alarmas, no se prohíbe el consumo de alimentos y bebidas y ninguna dependencia cuenta con aire acondicionado.	La infraestructura del Comité no cuenta con una buena señalización de las rutas de evacuación. Además no tiene avisos de advertencia sobre la prohibición del consumo de alimentos o fumar en espacios libres de humo. Es importante resaltar que las oficinas con gran cantidad de equipos de cómputo y el área de sistemas y tecnología no cuentan con un aire acondicionado, que prevenga un recalentamiento del sistema y mejore su desempeño.	**11 SEGURIDAD FISICA Y AMBIENTAL** 11.2.1 Emplazamiento y protección del equipo. El equipo debería situarse y protegerse para reducir el riesgo de materialización delas amenazas del entorno, así como las oportunidades de acceso no autorizado. 11.1.4 Protección contra amenazas externas y ambientales. Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.
No se cuentan con acuerdos de confidencialidad de la información.	Cualquier empleado puede guardar la información de la empresa en dispositivos personales externos del equipo de cómputo en el cual está trabajando como son USB, CDROM, Discos Duros Externos sin ninguna Restricción.	**GESTION DE ACTIVOS** 8.2.3 Manipulación de activos. Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados 8.3.1Gestión de medios removibles. Se deberían establecer procedimientos para la gestión de los medios informáticos removibles.

Fuente. Autor del Proyecto de Investigación

5. CONTROLES DE SEGURIDAD DE LA INFORMACION PARA EL COMITÉ DEPARTAMENTAL DE CAFETEROS DEL CAUCA.

Este informe se crea con el fin de aportar soluciones inmediatas a las inconsistencias que se presentan en el manejo de la información y la seguridad de las redes en el Comité Departamental de Cafeteros del Cauca.

Es importante resaltar que para un mayor acierto a la hora de generar recomendaciones, se estudió la norma ISO/IEC 27002:2013, que está organizada con base a 14 dominios, 35 objetivos de control y 114 controles[25], analizando y aplicando los controles requeridos en la Organización.

A continuación, se desarrolla la Política de Seguridad de la Información, para el Comité Departamental de Cafeteros de Cauca.

5.1.POLÍTICAS DE SEGURIDAD

Objetivo de Control. Documento de política de seguridad de la información

Control. La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes

La empresa debe contar con un documento que contenga las políticas de seguridad de la información, en el que se establezcan parámetros en los procedimientos, para garantizar la veracidad y disponibilidad de la información, además, la Dirección debe apoyar dichas políticas, con la publicación y difusión de las mismas a sus empleados.

El objetivo de las políticas de seguridad es implantar una serie de leyes, normas, estándares y prácticas que garanticen la seguridad, confidencialidad y disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos los miembros del Comité Departamental de Cafeteros del Cauca.

Cada elemento humano dentro de la organización es responsable de cada uno de sus actos, aun si tiene o no conciencia de las consecuencias.

5.2 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

Objetivo de control. Capacitación, educación y concientización en seguridad información

Control. Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y

[25]ISO 27000. ISO 27002. [en línea] Disponible en: http://iso27000.es/iso27002.html

actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Se creará una charla de capacitación para los empleados del Comité, Con el fin de informarlos, y motivarlos a seguir los lineamientos implantadosen las políticas de Seguridad de la organización.

Dicha capacitación, debe darse a los empleados al momento de comenzar a trabajar en el Comité, además se hace necesario realizar capacitaciones sobre el tema, cada 6 meses, para así, abarcar empleados antiguos y refrescarles las Políticas.

Cada empleado, contratista y/o aprendiz del Comité Departamental de Cafeteros del Cauca, debe conocer e implantar en su día laboral, todas y cada una de las políticas de seguridad de la Organización.

Es responsabilidad del Comité, capacitar el personal en la seguridad de la información, en sus roles, responsabilidades y obligaciones, durante la realización de sus labores; para reducir al máximo un el error humano en la empresa.

En caso de sospecha de incumplimiento por parte del empleado, se deberá realizar una verificación previa, antes de iniciar un proceso disciplinario. Si resulta que este es culpable, y fue apropiadamente capacitado, se hace necesaria la destitución inmediata de los deberes, derechos de acceso y privilegios.

5.3 GESTION DE ACTIVOS

Objetivo de Control. Inventario de Activos

Control. Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
Se debe contar con un documento donde se enumeren y se especifiquenlos activos de la información, dicho inventario debe contener elementos como: marca y modelo del computador, número de serie, unidades de disquete, unidades de disco duro, unidad de DVD/CD-ROM, tarjetas de sonido y de red, cantidad de RAM y cualquier otro detalle físico del computador o elemento de comunicación.

Objetivo de Control. Propiedad de los activos

Control. Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.

El inventario también debe contener, la ubicación física, la dependencia en la que se encuentra, el nombre del empleado, el usuario y la información de identificación de red (dirección IP, dirección MAC, subred, topología) e incluir la fecha de compra y la información acerca de la garantía.

A continuación, se presenta un estilo para la propiedad de los equipos de cómputo y el inventario de los mismos.

Tabla 10. Propiedad de los Equipos

HOJA DE CONTROL DE EQUIPOS			
DATOS PERSONALES			
Servidor o Estación de Trabajo			
Ubicación Física:			
Persona a Cargo			
No. De Serie:			
No. De Inventario			
No. de Equipo:		**Nombre**	
Dir. MAC		**Dir. IP**	
Máscara		**Dir. Proxy**	
Sistema Operativo			

CARACTERÍSTICAS DEL EQUIPO				
Elemento	**Marca**	**Descripción**	**Serial**	**No. Inventario**
Torre				
Procesador				
Memoria				
Disco Duro				
Tarjeta de Red				
Tarjeta de Video				
Monitor				
Teclado				
Mouse				
Parlantes				
Unidad de CD				
Unidad de Disquette				
Fuente: Autor del proyecto de Investigación				
Otros				

La siguiente tabla, presenta unmodelo de inventario de software para los computadores de la red del Comité. Incluyendo datos como el software del sistema operativo y aplicaciones. Para llevar a cabo el inventario de software, se necesita aplicar un formato como el siguiente; que permita recopilar la información relevante.

OBSERVACIONES

Fecha de Elaboración		**Elaborada Por:**	

Tabla 11. Inventario de Software

DATOS PERSONALES			
Servidor o Estación de Trabajo			
Ubicación Física:			
Persona a Cargo			
No. De Serie:			
No. De Inventario			
No. de Equipo:		**Nombre**	
Dir. MAC		**Dir. IP**	
Máscara		**Dir. Proxy**	
Sistema Operativo			

SOFTWARE INSTALADO				
Nombre	**Versión**	**Descripción**	**Fecha Instalación**	**Fecha Actualización**
Otros				

OBSERVACIONES			
Fecha de Elaboración		**Elaborada Por:**	

Fuente: Autor del proyecto de Investigación

Objetivo de Control. Manipulación de activos.

Control. Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados

Cada usuario debe manejar una identificación única que no puede compartir o dar a conocer a otras personas, Además los usuarios no deben cambiar la configuración de los equipos, en caso de que lo hagan, pueden provocar una gran cantidad de trabajo adicional para el personal de mantenimiento de la red.

No se permite almacenar información personal o ajena a la entidad en las estaciones de trabajo.

Objetivo de Control. Gestión de medios removibles.

Control. Se deberían establecer procedimientos para la gestión de los medios informáticos removibles

Todo documento en formato digital, debe presentar una clasificación correspondiente, se va a catalogar la información como "Publica" o "Privada", según el nivel de confidencialidad que esta requiera.

La información en formato digital, clasificada como "Privada", debe ser encriptada, cuando es almacenada en cualquier medio (CD´s, Disco Duro, USB, etc.).

Los usuarios deben tener cuidado con la confidencialidad de la información. Todo documento catalogado como "Publico" puede ser almacenado en cualquier medio, másse debe tener sumo cuidado con la información "Privada", pues esta representa un alto valor para la organización,

El acceso a la información clasificada como "Privada" debe ser autorizado por el jefe inmediato del empleado o la persona encargada de la dependencia, además toda autorización extra curricular debe ser documentada en formato físico.

Respecto al almacenamiento de las copias de seguridad estas se pueden realizar en cualquier momento o cuando el administrador del sistema lo crea conveniente. Y las realizara el administrador desde una maquina cliente o servidor, si se decide realizar las copias de seguridad en Cd's, USB o Cualquier otro disco extraíble, este debe ser guardado bajo llave, de manera restringida.

5.4 CONTROL DE ACCESOS.

Objetivo de Control. Gestión de los derechos de acceso asignados a usuarios

Control. Se debería asegurar el acceso de usuarios autorizados a fin de prevenir el acceso no autorizado a los sistemas y servicios.

Cada empleado debe ser registrado en los sistemas de información el Comité, se le asignara un usuario y una contraseña única e intransferible, según la dependencia en la que ejerza sus funciones. Este acceso será habilitado desde el momento en el que comience a laborar en la organización y en el caso de terminación de contrato, se inhabilitara su usuario y se le restringirá el derecho de acceso. Todo cambio de estado, deberá quedar en los registros del control de acceso.

El administrador del sistema será el encargado de crear los usuarios (login y password) para cada trabajador y autorizar el acceso según el rol que desempeñen en la organización.Conel fin de evitar que personas ajenas al sistema hagan uso de él.

Los password no deben visualizarse en el momento en que se digitan y deben ser almacenadas de forma encriptada. No es permitido utilizar nombres personales, fechas o demás características identificables con el usuario. Y debe estar conformado por 8 caracteres preferiblemente combinación de letras y números y será escogido por el usuario.

Objetivo de Control. Gestión de los derechos de acceso con privilegios especiales.

Control. Se debería restringir y controlar la asignación y uso de los privilegios de usuario en cada equipo de cómputo**.**

El uso de los sistemas de información del Comité Departamental de Cafeteros del Cauca, debe ser limitado y controlado por el administrador de los mismos, los derechos de acceso con privilegios especiales, serán asignados a personal capacitado, la autorización y la asignación de privilegios es deber del administrador, esto se hace con el fin de evitar accesos no autorizados, que lleguen a afectar, modificar o manipular la información.

Objetivo de Control. Autenticación de usuario para conexiones externas.

Control. Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios.

Es labor del personal de sistemas monitorear los accesos a los mismos, con el fin de evaluar riesgos y controlar al acceso de usuarios remotos, en especial para redes inalámbricas

Las conexiones remotas deberán realizarse por medio de un equipo de cómputo seguro. Para esto es necesario contar con la identificación de cada equipo del Comité, con el fin de determinar a qué red está conectado y si tiene los permisos necesarios para acceder a ella.

Los accesos al sistema deben ser monitoreados regularmente por el Jefe del área de Sistemas o el administrador de los sistemas de información, además es necesario que exista un reporte de ubicación y fecha exacta en la que se accede a la aplicación, para controlar al

máximo las conexiones externas del personal del Comité en horarios no autorizados, las conexiones remotas deberán realizarse por medio de un equipo de cómputo seguro y solo lo pueden hacer, empleados con privilegios especiales.

5.5 SEGURIDAD FÍSICA Y AMBIENTAL

Objetivo de Control. Controles físicos de entrada.

Control. Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado

Para el acceso a los sitios y áreas restringidas se deben implementar medidas de seguridad físicas para certificar la integridad de las oficinas. Las medidas de protección deben ser de acuerdo al nivel de importancia que maneje la información procesada y almacenada en las oficinas.Las áreas de seguridad deberán estar protegidas con las barreras y controles físicos contra acceso no autorizado, daño, robo, o cualquier tipo de manipulación que ponga en riesgo la información o cualquier otro activo de las oficinas del Comité.

Es importante que los visitantes cuenten con un acompañamiento que les indique hacia donde deben dirigirse, según lo requiera.

Objetivo de Control. Seguridad de oficinas, despachos y recursos.

Control. Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.

El Jefe del área de Sistemas, debe encargarse de tomar las medidas necesarias para mantener la seguridad de las diferentes oficinas.Las oficinas deben contar con una señalización que reduzca al máximo la entrada equivocada a sitios con restricción por parte del personal visitante. Es importante que se lleve un registro de entrada a las áreas restringidas o en las que su nivel de seguridad sea medio/alto. Para el ingreso del personal, se debe llenar una ficha como el modelo que veremos a continuación, y en algunos casos se debe presentar una carta de autorización de entrada.

Tabla 12. Registro de entrada

ID	Fecha	E/V	Nombre	Motivo	Firma
1	__/__/__				
2	__/__/__				
3	__/__/__				
4	__/__/__				
5	__/__/__				

Fuente: Autor del proyecto de Investigación

E/V=Empleado/Visitante

El acceso al cuarto de comunicaciones sólo se permite al personal asignado y autorizado por el jefe del área de sistemas.

Objetivo de Control. Protección contra las amenazas externas y de origen ambiental.

Control. Se debe designar y aplicar medidas de protección física contra incendios, inundación, terremoto, explosión, malestar civil y otra forma de desastre natural o humano

Es importante que materiales peligrosos, como combustibles, sean almacenados a una distancia prudente del área asegurada. Implementar extintores debidamente recargados y probados, además de contar con detectores de calor y humo.

Con el fin de evitar inundaciones se debe contar con diferentes niveles del suelo, barreras, desagües y pisos falsos, para evitar el rápido avances del agua a las oficinas.

El cableado de la red de datos debe estar aislado del cableado eléctrico por canaletas. Se recomienda realizar estas instalaciones con base a la norma técnica.

Se deberá prestar cuidado a cualquier amenaza contra la seguridad presentada por estructuras vecinas. Así como también contar con alarmas de detección de intrusos, que emitan previo aviso a las autoridades.

En cuanto a factores ambientales, se deben evitar contaminantes para los computadores como el polvo y evitar las altas temperaturas. Ya que el número de computadores por oficina es tan elevado, se hace necesario implementar aires acondicionados que regulen la temperatura y eviten el re-calentamiento de los mismos.

No se permite comer, beber o fumar cerca de los equipos de cómputo y/o de oficina.

Objetivo de Control. Emplazamiento y protección del equipo.

Control. El equipo debería situarse y protegerse para reducir el riesgo de materialización delas amenazas del entorno, así como las oportunidades de acceso no autorizado.

Se debe proteger el equipo con un buen sistema de puesta a tierra, y se debe contar con sistemas de alimentación ininterrumpida (UPS) para evitar que el equipo deje de funcionar cuando se producen interrupciones del suministro eléctrico.

Los equipos que manejan datos confidenciales deberán ubicarse fuera de vista de personas no autorizadas.

Objetivo de Control. Mantenimiento de los equipos.

Control. Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.

Para tener un buen funcionamiento de los equipos se deben realizar mantenimientos preventivos por lo menos, una vez, cada trimestre. Además el personal de sistemas debe estar disponible cada vez que un equipo de cómputo lo requiera.

Es necesario mantener un registro de todas las reparaciones que se realice alosequipos. Esto permitirá predecir problemas futuros con el hardware y el software.

A continuación, Se muestra un ejemplo de formato que debe ser aplicado en el Comité, para el registro de mantenimiento.

Tabla 13. Registro de Mantenimiento

REGISTRO DE MANTENIMIENTO			
Servidor o Estación de Trabajo			
Ubicación Física:			
Persona a Cargo			
No. De Serie:			
No. De Inventario			
No. de Equipo:		**Nombre**	
Dir. MAC		**Dir. IP**	
Máscara		**Dir. Proxy**	
Sistema Operativo			
Tipo de Reparación	**Hardware**		**Software**
Descripción del Problema			
Descripción de la Reparación			

OBSERVACIONES			
Fecha de Elaboración		**Elaborada Por:**	

Fuente: Autor del proyecto de Investigación

Objetivo de Control. Políticas de puesto de trabajo despejado y pantalla limpia.

Control. Políticas para escritorios y monitores limpios de información.

Es importante el hecho de no tener información trascendental en la pantalla principal del computador. Como también se recomienda no tener información física sobre el escritorio, al alcance de personas no autorizadas.

Cada usuario debe mantener en su equipo un protector de pantalla, protegido por contraseña que se active cuando se aleja del computador o dure al menos 2 minutos sin usarlo.

No se debe almacenar información personal o ajena a la entidad en las estaciones de trabajo. Para esto se debe aplicar un programa que congele el Windows del equipo, controlando cualquier modificación, instalación o desinstalación de software; este volverá a su estado inicial (Estado de Congelación) al momento de reiniciar el computador.

5.6 SEGURIDAD EN LA OPERATIVA.

Objetivo de Control. Protección contra código malicioso.

Control. Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.

Para la protección contra código malicioso se hace necesario que cada computador cuente con un antivirus actualizado que permita escanearlo periódicamente para evitar virus que afecten el funcionamiento del equipo o el desempeño de la red.

El personal autorizado debe capacitar a los funcionarios del Comité, para que hagan revisiones periódicas sobre el buen funcionamiento de su antivirus. Con el fin de minimizar al máximo la entrada de software’s maliciosos que afecten, impidan o roben le información.

Los antivirus que se instalarán en los servidores y los equipos de la organización deben ser licenciados, y configurados para actualizaciones diarias.

Todos los archivos recibidos por medios externos o adjuntos a través del correo electrónico deben ser revisados por el antivirus antes de ejecutarlo. Con el fin de detectar, eliminar y prevenir la implantación de código malicioso.

En caso de detectarse fallas en el funcionamiento de los antivirus, éstas deben ser comunicadas al Jefe del Área de Sistemas, para una respectiva verificación.

Es importante que los empleados sean conscientes de que el descargue y la instalación de software no licenciados es prohibida. De hallarse software ilegal en alguna dependencia, será reportado como incidente de seguridad y se tomarán medidas de precaución necesarias. La responsabilidad de informar a los empleados sobre esta restricción es del Jefe de Sistemas o el personal asignado por el mismo.

Objetivo de Control. Copias de seguridad de la información.

Control. Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación.

Se deben realizar copias de seguridad de la base de datos, estas copias de seguridad servirán de respaldo y/o para la recuperación en casos de perdida de información.

Las copias de seguridad deben ser realizadas por los funcionarios del Comité, con una frecuencia diaria y el administrador del sistema debe hacer revisión de copias de seguridad, al menos semanalmente y serán realizadas desde una maquina cliente o servidor. Además el Jefe del área de Sistemas puede considerar la opción de realizar backup’s remotos bajo una multiplataforma de alto rendimiento.

5.7 SEGURIDAD EN LAS TELECOMUNICACIONES.

Objetivo de Control. Controles de red.

Control. Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.

Antes de conectar cualquier equipo a la red, es responsabilidad del personal de Sistemas asegurarse de revisarlo y posteriormente registrarlo en la red del Comité, con el fin de proteger y monitorear el tráfico de datos, controlando y detectando actividades inusuales en los nodos de la red.

El registro de cada componente de red, consiste fundamentalmente en la documentación y señalización de los componentes físicos, para esto se debe establecer una nomenclatura de

documentación para los distintos componentes a señalizar. Todos los cables, paneles y salidas deben estar etiquetados tanto a simple vista como en su interior, con el fin de identificar los diferentes elementos que conformarán la red.

Además se debe identificar cada área de la entidad, como el siguiente ejemplo.

Tabla 14. Identificación de Dependencias

NOMBRE	ABREVIATURA
Oficina de Sistemas	OS
Sica	SICA
Dirección Ejecutiva	DE
Dirección Administrativa	DA
Secretaría	SE
Contaduría y Pagaduría	CP
Créditos	CR
Trabajo Social	TS
Obas Civiles	OB
Archivo	AR
Seccional Popayán	SP
Servicio Técnico	ST
Extensión	EX
Recepción	RE

Fuente: Autor del Proyecto de Investigación

Según la norma EIA/TIA-606 (Administration Standards for the Telecommunications Infrastructure of Commercial Building), que presenta las guías para marcar y administrar los componentes de un Sistema de cableado estructurado, se deben identificar los puntos lógicos, con las siguientes indicaciones.

Los puntos lógicos se identificarán de acuerdo al siguiente código.

Tabla 15. Identificación de Puntos Lógicos

IDENTIFICACION DEL AREA	ABREVIATURA (Máximo 2 caracteres)
Rack	La letra R y un dígito
Panel	La letra P y un dígito
Puerto	La letra PT y dos dígitos

Fuente. Autor del Proyecto de Investigación.

Tabla 16. Etiqueta de los puntos lógicos

RE/R1/P1/PT01

Fuente. Autor del Proyecto de Investigación.

En el ejemplo anterior RE identifica la dependencia (Recepción), R1 identifica el rack 1, P1 al panel 1 y PT01 es el punto número 1 de dicha oficina.

La numeración de los puntos lógicos en cada oficina se hará en forma consecutiva en el sentido contrario a las manecillas del reloj, además, de la identificación por código se recomienda que las tomas presenten una identificación por color de acuerdo al servicio que preste: color rojo para los servicios de voz y azul para los servicios de datos.

Los elementos del rack deben contar con una identificación clara, Los Patch panel deben estar identificados de la siguiente manera:

Panel: La letra P y un dígito.
Rack: La letra R y un dígito.

Tabla 17. Etiqueta de un Patch panel

R1/P1

Fuente. Autor del Proyecto de Investigación.
En el ejemplo anterior R1 identifica el rack 1 y P1 al panel 1.

La identificación de los switches se realizará de manera similar:

Switch: La letra S y un dígito.
Rack: La letra R y un dígito.

Tabla 18. Etiqueta de Switch

R1/S1

Fuente. Autor del Proyecto de Investigación.

Todos los elementos activos de la Red deben presentar en la parte anterior de su chasis la identificación de la dirección MAC y su serial con el fin de facilitar su administración.
Las tomas eléctricas reguladas deben ir identificadas con el número del circuito a que pertenece y en la parte posterior de la puerta del tablero eléctrico debe ir el plano de los circuitos instalados.

CONCLUSIONES

Se realizó el reconocimiento del Comité Departamental de Cafeteros del Cauca, identificando su objetivo principal, estructura orgánica y procesos en el manejo de la información. Al realizar el diagnóstico se detectaron fallas físicas, en el control de acceso, en la infraestructura y en el cableado estructurado, entre otras. También fueron encontradas una serie de fallas lógicas en la protección de los datos, el manejo de los procesos de la información y los accesos no autorizados, que generan problemas de seguridad de la información.

Para el análisis acertado de la Seguridad de la Información, se tomó como base la norma ISO/IEC 27002, que establece lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información dentro de una organización, ya que esta genera gran cantidad de buenas prácticas que son de gran provecho en la seguridad de la información del Comité Departamental de Cafeteros del Cauca ayudándole a cumplir los requerimientos de la organización de una manera eficaz y estable.

Posteriormente al análisis de la NTC-ISO/IEC 27002, se genera un documento que proporciona una guía a seguir para la seguridad de la información en el Comité de Cafeteros. En este se toman siete dominios de la norma (Política de Seguridad, Seguridad ligada a los Recursos Humanos, Gestión de Activos, Control de Accesos, Seguridad Física y Ambiental, Seguridad en la Operativa y Seguridad en las Telecomunicaciones), que aplican a las fallas que tiene el Comité en relación a la seguridad, si estos controles son implementados, se consigue minimizar los riesgos a los que está expuesta la Información de la organización.

RECOMENDACIONES

Presentar a los directivos del Comité Departamental de Cafeteros del Cauca, este análisis de la norma ISO/IEC 27002 con respecto al manejo de la información.

Para su aprobación e implementación, se recomienda a los directivos del Comité, estudiar el documento en presencia del Jefe del área de Sistemas.

Es importante aplicar las políticas nombradas en el desarrollo del proyecto, y que se cumplan en su totalidad.

En conjunto con el personal del área de Sistemas, se debe organizar una serie de capacitaciones periódicas, que formen e informen a los empleados del Comité, sobre las políticas del manejo de la información. Así mismo, se debe crear un acuerdo de confidencialidad de la información privada, donde todo el personal pueda conocer sus responsabilidades y sanciones en caso de faltar al acuerdo y ocasionar un nivel de riesgo en la organización.

Se deben establecer claramente los roles y asignar responsabilidades a empleados del Comité. También es necesario implementar formatos para mantener un inventario actualizado de todos los activos (Hardware y software, equipos de oficina y comunicaciones, archivos y backup’s) con los que se cuenta.

Se deben implantar controles de acceso físico y lógico en cada dependencia del Comité, especialmente a las áreas restringidas o que manejen un alto grado de privacidad de la información. Además, es necesario cuidar la seguridad ambiental de las amenazas externas, como implementar extintores, debidamente recargados y ubicados en lugares ventajosos para todo el personal e instalar aires acondicionados en las oficinas que tengan más de cuatro equipos de cómputo, con el fin de prevenir un recalentamiento de los mismos.Las gradas, deben ser seguras y con los controles respectivos como antideslizantes y barras de apoyo sobre la pared para sujetarse

Se debeproteger la información contra códigos maliciosos, implementando controles de prevención, como la utilización de antivirus actualizados. Sin embargo es de vital importancia que se realicen copias de seguridad a una frecuencia diaria o en su defecto semanal, para minimizar cualquier tipo de pérdida de la información.

Es responsabilidad del empleado, proteger su equipo de cualquier acceso no autorizado, para esto, debe asegurarse de que el equipo tenga la protección apropiada, como la activación automática de un protector de pantalla después de cierto tiempo de inactividad. Además se debe tener en cuenta, que un equipo desatendido es un área de trabajo desatendida, por lo que se debe mantener una política de escritorios limpios, donde el área de trabajo debe permanecer libre de documentos a los cuales una persona no autorizada podría tener acceso.

Es importante resaltar que cualquier tipo de falla, debe ser inmediatamente corregida, pero también registrada y analizada para que sirvan en la toma de decisiones y para realizar acciones necesarias.

Se recomienda aplicar y hacer cumplir las políticas mencionadas en el desarrollo de este proyecto, con el fin, de reducir cualquier riesgo a la cual pueda estar expuesta la información del Comité.

REFERENCIAS BIBLIOGRÁFICAS

LAMILLA RUBIO, Erick A.; PATIÑO SANCHEZ, José R. y MARTIN M, Ivonne. Desarrollo de políticas de seguridad en implementación de cuatro dominios en base a la norma 27002 para el área de hardware en la empresa UniplexSystems S.A. en Guayaquil. Disponible en la web y de acceso libre. Facultad de Ingeniería en Electricidad y Computación "FIEC". Escuela Superior Politécnica del Litoral "ESPOL", Ecuador.

BUITRAGO ESTRADA, Johanna Carolina; BONILLA PINEDA, Diego Hernando y MURILLO VARON, Carol Estefanie. Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - sgsi, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001. Disponible en la web y de acceso libre. Universidad EAN, Bogotá. 2012.
http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

MUÑOZ SERNA, Rodrigo y MARTINEZ ARIAS, Mario Alberto. Caracterización de Procesos de Gestión de TI basados en COBIT 5 y mapeo con ISO27002, ITIL, CMMI DEV, PMBOK, para la implementación en la industria Editorial Colombiana, apoyando el proceso de transformación digital. Disponible en la Web y de acceso libre. Universidad ICESI, Santiago de Cali. 2012.
https://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/70260/1/caracterizacion_proceso_gestion.pdf

FRANCO, Diana C. y GUERRERO, Cesar D.Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002. Disponible en la Web y de acceso libre. Universidad de los llanos, Villavicencio; Universidad Autónoma Bucaramanga, Colombia. Agosto de 2013.
http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf

PASTOR I COLLADO, Joan Antoni. Concepto de Sistema de Información en la Organización. Editorial UOC 2OO2.

SERRANO CEDILLOS, Leticia Esmeralda. El rol de la auditoria computarizada como herramienta de confiabilidad en la información contable. Universidad Dr. José Matías Delgado, antiguo Cuscatlan. El Salvador, Centroamérica. Noviembre, 2006.

REPÚBLICA DE COLOMBIA, Constitución Política De La República De Colombia De 1991,Actualizada hasta el Decreto 2576 del 27 de Julio de 2005 Constitución política de Colombia. De la protección de la información y de los datos, Ley 1273 de 2009 [En Línea] Disponible en internet:
http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm

LOBO PARRA, Leonard David; OVALLOS OVALLOS, JesusAndres y SIERRA GOMEZ, Ana Maria. Plan de gestión de la seguridad de la información de la biblioteca Argemiro Bayona de la Universidad Francisco de Paula Santander Ocaña, mediante la aplicaion de la norma iso 27001 y técnicas ethical hacking. Universidad Francisco de Paula Santander Ocaña. Diciembre, 2013. Disponible en: http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/325/1/25095.pdf

MOLINA RINCON, Erica Lorena; RODRIGUEZ ALVAREZ, Oscar Humberto; SANCHEZ DELGADO, Yalide y VERGEL NUÑEZ, John Alexander. Guía para la seguridad basada en la norma iso/iec 270002, para la dependencia división de sistemas de la Universidad Francisco de Paula Santander Ocaña. Universidad Francisco de Paula Santander Ocaña. Julio, 2014. Disponible en: http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/439/1/25830.pdf

MARULANDA PADILLA, Henry. Evaluacion mediante el estándar ISO 27001 de la seguridad física y lógica de la infraestructura tecnológica de la clínica San Jose S.A.S de la ciudad de Barrancabermeja. Barrancabermeja Santander. Julio 2014. Disponible en: http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/180.

FEDERACION NACIONAL DE CAFETEROS. Quienes somos (en linea) Disponible en: http://www.federaciondecafeteros.org/particulares/es/quienes_somos

FEDERACION NACIONAL DE CAFETEROS. Comites departamentales (en linea). Disponible en: http://www.federaciondecafeteros.org/particulares/es/nuestros_caficultores/comites_departamentales/

FEDERACION NACIONAL DE CAFETEROS. Comité de cafeteros del cauca (en linea) Disponible en: http://cauca.federaciondecafeteros.org/fnc/nuestro_comite/

ISO 27000. ISO 27002. [en línea] Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO 27000. ISO/IEC 27002. [en línea] Disponible en: http://www.iso27000.es/iso27000.html

ISO 27000. Dominios de la ISO 27002:2013. [en línea] Disponible en: http://iso27000.es/download/ControlesISO27002-2013.pdf

AUDITORIA DE SISTEMAS. Riesgos Informaticos. [en línea] Disponible en: http://auditoriadesistemas.galeon.com/productos2223863.html

ANEXOS

ANEXO A. Encuesta dirigida a los empleados del Comité Departamental de Cafeteros del Cauca.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS

Objetivo: Obtener información acerca de la necesidad de implementar controles de seguridad de la información en el Comité Departamental de Cafeteros del Cauca.

1. El comité departamental de cafeteros del cauca cuenta con políticas de seguridad de la información?

   Si ___ no ____ No sabe ___ no contesta___

2. En el comité realizan revisiones constantes a intervalos planificados en el manejo de la información para garantizar que ese manejo es adecuado, eficaz y suficiente?

   Si ___ no ____ No sabe ___ no contesta___

3. La empresa cuenta con el personal idóneo en el área de sistemas?

   Si ___ no ____ No sabe ___ no contesta___

4. Los equipos de sistemas cuentan con protección contra las amenazas físicas y ambientales?

   Si ___ no ____ No sabe ___ no contesta___

5. La organización tiene establecido políticas de control de acceso a diferentes dependencias especialmente la de sistemas?

   Si ___ no ____ No sabe ___ no contesta___

6. La empresa reporta los Incidentes de Seguridad de la Información que se presenten?

   Si ___ no ____ No sabe ___ no contesta___