Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca

Adopt an information security policy based on an NTC ISO / IEC 27002: 2013 standard for the Codelcauca Cooperative

Yiner Ramos[1], Orlando Urrutia[2], Dayner Ordoñez[3], Alberto Bravo[4]
[1,2,3,4]Institución Universitaria Colegio Mayor del Cauca
[1]ramosyiner@unimayor.edu.co, [2]urreaorlando@unimayor.edu.co, [3]dordonez@unimayor.edu.co, [4]abravo@unimayor.edu.co

Resumen–*El desarrollo del presente proyecto denominado "Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la cooperativa CODELCAUCA", tiene como objetivo principal la adopción e implementación de políticas de seguridad de la información teniendo en cuenta la norma 27002:2013, las cuales servirán como guía para proporcionar herramientas que contribuyan a mejorar la gestión de la información obtenida, generada o procesada en CODELCAUCA., la política de seguridad facilitará la adopción de lineamientos necesarios para garantizar la seguridad de la información teniendo las directrices establecidas en los objetivos de control 5.1.1 y 5.1.2 relacionados con políticas de seguridad y sustentados en los objetivos de la empresa. Teniendo en cuenta este planteamiento se tendrá presente los procesos y procedimientos, como: registro de incidencias, respaldo de la información, registro de incidencias, respaldo de la información, mantenimiento de equipos y copias de seguridad. Para los cuales se partirá teniendo en cuenta los criterios relacionados con política de seguridad, gestión de activos, control de acceso, seguridad física y ambiental, seguridad relacionada con el personal, teniendo en cuenta los dominios establecidos en el anexo A de la NTC ISO/IEC 27001:2013. Finalmente hay que destacar que este trabajo se desarrolla entre la Institución Universitaria Colegio Mayor del Cauca y el la Cooperativa Codelcauca, en un proceso de integración de la academia con el sector productivo de la ciudad de Popayán.*

Palabras claves–*Dominio, norma, objetivos de control, procesos, política de seguridad, activos informáticos, anexo A.*

Abstract–*The development of this project called "Adopting an information security policy based on a standard domain of NTC ISO/IEC 27002: 2013 standard for CODELCAUCA cooperative", has as main objective the adoption and implementation of information security policies having 27002: 2013, which will serve as a guide to provide tools that contribute to improve the management of information obtained, generated or processed in CODELCAUCA., The security policy will facilitate the adoption of guidelines necessary to guarantee the security of the Information having the guidelines established in the control objectives 5.1.1 and 5.1.2 related to security policies and sustained in the objectives of the company. Considering this approach will consider the processes and procedures, such as: record of incidents, backup of information, record of incidents, backup of information, maintenance of equipment and backups. For which it will be divided considering the criteria related to security policy, asset management, access control, physical and environmental security, personnel related security, considering the domains established in Annex A of the NTC ISO / IEC 27001: 2013. Finally, it should be noted that this work is carried out between the University Institution Colegio Mayor del Cauca and the Codelcauca Cooperative, in a process of integration of the academy with the productive sector of the city of Popayan.*

Keywords– *Domain, standard, control objectives, processes, security policy, Computer assets, Annex A.*

1. Introducción

La seguridad de informática ha juega un papel importante en el desarrollo empresarial del momento, en tal sentido las empresas independientemente del tipo de servicio que ofrezcan a la sociedad tienen que salvaguardar su información y es en este punto en el cual la seguridad informática juega un papel importante. En este sentido la información no solo debe ser referido como un problema tecnológico, sino también organizativo y de gestión para afrontar las amenazas desde diferentes puntos de referencia en el cual la tecnología juega un papel importante, en este sentido la adopción e implementación de políticas de seguridad de la información en CODELCAUCA no solo es responsabilidad de algunas áreas, como por ejemplo la división de sistemas, sino que debe corresponder a un esfuerzo colectivo que involucre a toda la organización. De este modo el éxito de este proyecto del proyecto depende de la forma como se unan esfuerzos para mantener colectivamente la información, es decir de un esfuerzo corporativo.

Para alcanzar este propósito es importante ceñirse a una norma, que garantice el mantenimiento de la integridad de la información, la ISO 27002[1] proporciona los objetivos de control y controles aplicados a política de seguridad, seguridad de los recursos humanos, gestión de activos, seguridad física y ambiental entre otros dominios los cuales serán desarrollados en este documento.

En el propósito por mantener la confidencialidad, la integridad y la disponibilidad de la información, se pone nuevamente de manifiesto el compromiso de la corporación [2] y en consecuencia involucra a todos las dependencias que la constituyen, como son: la división de sistemas, talento humano, planeación, control interno, alta gerencia. Por consiguiente la seguridad de la información es un proceso que va desde la gestión de riesgo, el proceso de ingeniería de la seguridad, hasta el aseguramiento. Por lo que este proyecto se sustenta en las primeras etapas del ciclo de madurez del sistema en relación con el análisis de madurez de la seguridad informática en COODELCAUCA y hay que seguirlo desarrollando e impulsando para irlo mejorando y madurando.

Teniendo en cuenta lo anterior se puede decir que no hay un sistema 100% seguro. La seguridad de la información se sustenta en tres características importantes [3] como son, la integridad, la confidencialidad y disponibilidad de la información., elementos sustanciales para el aseguramiento de la información en CODELCAUCA.

Para adoptar e implementar una política de seguridad de la información en una empresa como CODELCAUCA, es necesario partir de una evaluación obtenida de la aplicación de instrumentos como encuesta y entrevistas que nos proporcione información en relación como las diferentes dependencias participan para garantizar el aseguramiento de la información teniendo en cuenta la razón de ser de la empresa analizada en este caso. De manera general lo que se busca garantizar las políticas de seguridad a partir de los dominios definidos en el Anexo A teniendo en cuenta los dominios definidos para este caso y la aplicación de objetivos de control y controles definidos en la norma.

Teniendo en cuenta lo anteriormente planteado, es importante para una empresa del sector financiero como es CODELCAUCA, generar una dinámica para lograr un robusto sistema de información, el cual debe ser permanente revisado para garantizar el aseguramiento de este sistema de información, por lo que es de gran importancia aplicar los objetivos de control y controles relacionados con el mantenimiento de su sistema de información.

2. Planteamiento del problema

La cooperativa Codelcauca cuenta con un equipo humano, con una tecnología y unos activos que hoy en día almacenan, transportan y procesan información que facilitan la prestación del servicio en el sector financiero, para lo cual se manejan una gran cantidad de documentos, inherentes a lo establecido en su misión y visión, a través de los cuales se fortalecen día a día los procesos de negocio, entre los cuales se pueden mencionar informes presupuestales, contratos y e información financiera de sus clientes en las diferentes sedes de la misma.

Sin embargo está información puede ser afectada de alguna manera, es decir los activos informáticos, la seguridad física y ligada a los recursos humanos entre otras están sometidos a amenazas que van desde el fraude electrónico, hasta ataques de denegación de servicios, otros. Lo cual puede conllevar a que la información sea manipulada, suplantada, borrada y que de alguna u otra forma se afecte la legitimidad, prestigio

y el buen nombre de la empresa incluso, podría ocasionar serios inconvenientes legales.

Para contribuir en el proceso de aseguramiento de la información, se propone el proyecto "Diseño de una política de seguridad de la información basada en un dominio del estándar NTC ISO/IEC 27002:2013 que permite la creación de una política de seguridad que permitirá evitar y mitigar los posibles riesgos a los que pueden estar expuestos tanto los sistemas de información con los que cuenta la empresa, como los mismos datos y contribuir de esta manera a mantener la integridad de la misma.

3. Norma ISO/IEC 27002

El origen de la ISO/IEC 27000 que tiene como propósito proporcionar criterios y soporte orientado a garantizar la seguridad de la información, en el año 2002 se hizo la revisión de lo que en ese momento constituyo la ISO 27001 como norma que permite el aseguramiento, la confiabilidad y la integridad de datos e información y su procesamiento [4].
En 2007, se incorpora la ISO 27002, la cual se describe en términos de objetivos de control y controles aplicados a la seguridad de la información, la versión de esta norma en el año 2013 es la ISO/IEC 27002:2013, la cual está conformada por 35 objetivos de control 114 controles y 14 dominios [5].
La información como activo es de gran importancia para cualquier empresa y en nuestro caso particular para la empresa CODELCAUCA, por lo que es un objetivo de primer orden asegurar dicha información y de igual manera la tecnología utilizada en su procesamiento.
En este sentido este sentido se debe implantar en CODELCAUCA un sistema que permita la adecuada gestión, organización y aseguramiento de la información como un proceso cuidadoso, documentado y sustentado en objetivos de seguridad informática. en este proyecto se abordan directrices establecidos en los numerales 5.1 y 5.2 de la norma ISO 27002 relacionado con políticas de seguridad y relacionado con los objetivos de la empresa, al incluir procesos y procedimientos como registro de incidencias, respaldo de la información, mantenimiento de los equipos, restauración de copias de seguridad.
Esto permitió establecer un campo de acción sustentado en cinco dominios de la norma ISO/IEC 27002:2013, como son política de seguridad, gestión de activos, control de acceso, seguridad física y ambiental y seguridad relacionado con el personal. El desarrollo del proyecto en este sentido se sustenta en la aplicación de instrumentos de medida como entrevista y encuesta aplicado a los empleados de la empresa y relacionados con la gestión, procesamiento y aseguramiento de la información.

4. Infraestructura tecnológica de Codelcauca [6]

CODELCAUCA, es una empresa de servicios financieros cuya oficina principal está ubicada en la ciudad de Popayán, además cuenta con sucursales en las ciudades del Bordo y Santander de Quilichao, estas sedes se comunican entre sí haciendo uso de una red y a través de la infraestructura de Internet, a través de dicha comunicación buscan mejorar en la prestación del servicio financiera en estas ciudades del departamento del Cauca. La figura 1, ilustra la topología de red de CODELCAUCA en la cual se indica cómo están conectadas las sedes del Bordo y Santander de Quilichao con la sede Popayán.

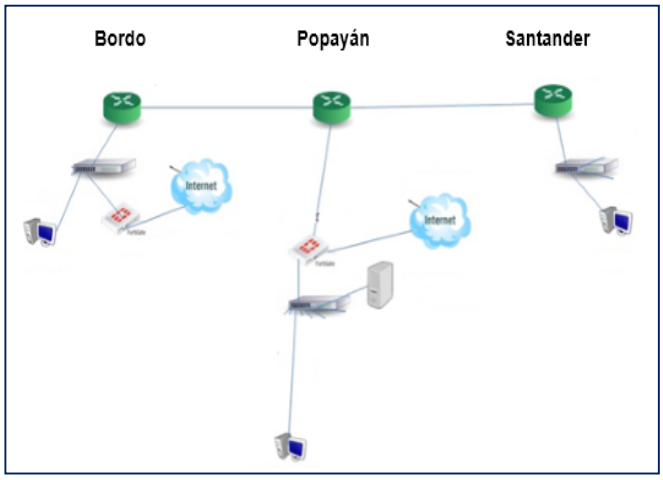


Figura 1. Mapa de red de CODELCAUCA.

Para una adecuada prestación de los servicios financieros COODELCAUCA cuenta con aplicaciones y herramientas software suministradas por un proveedor de internet, utilizando un servicio externo de Microsoft azure. La figura 2 relaciona las diferentes aplicaciones software utilizadas por esta empresa del sector financiero.

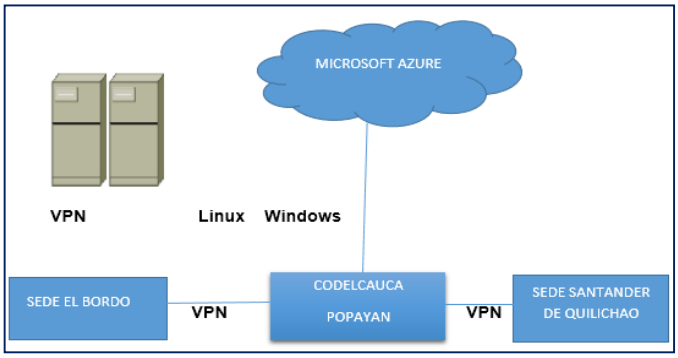


Figura 2. Servicio externo de servidores.

Para las actividades tecnológicas de comunicación y de la información, en su modelo de negocio utiliza la herramienta software denominada Linix software para el desarrollo de las actividades financieras. Una interfaz de la aplicación se ilustra en la siguiente figura 3.

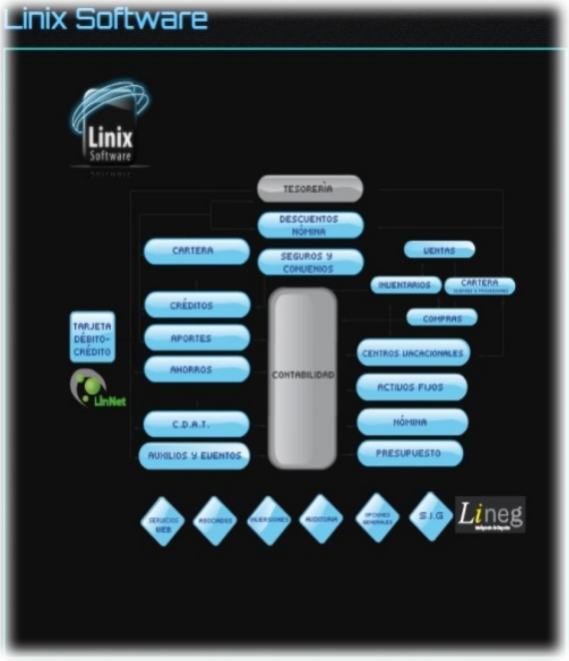


Figura 3. Core bancario CODELCAUCA.

5. Adopción de la norma ISO/IEC 27002:2013

Para el análisis de los dominios definidos para trabajar en el desarrollo del proyecto se aplicaron entrevistas y encuestas para extraer la información necesaria y determinar la vulnerabilidad de la red de datos de CODELCAUCA. Una vez obtenida dicha información realizo su procesamiento, el cual se indica más adelante en este documento.

En la implementación y adopción de la política de seguridad de la información en la empresa se involucró al jefe de la división de sistemas y 22 funcionarios más de diferentes dependencias que conforman el grupo de trabajo que interactúa y maneja información diariamente en sus diferentes puestos de trabajo.

La recolección de información es de vital importancia en la realización del proyecto del proyecto, teniendo en cuenta la revisión documental de la norma, encuestas, entrevistas, listas de chequeo como elementos de apoyo a la política de seguridad de la empresa COODELCAUCA y de esta forma contribuir en el mantenimiento e integridad de la información. De manera general la aplicación de los instrumentos de encuesta y entrevista se aplican al jefe del área de sistemas [7] y personal relacionado con el manejo de información para tener información relacionada con: política de seguridad, activos informáticos, control de acceso, seguridad física y ambiental y seguridad relacionada con el personal. Los cuales se describen muy rápidamente a continuación.

5.1 Política de seguridad

La política de seguridad plantea que los diferentes dominios son de vital importancia para mantener la integridad de la información y el desarrollo de un estudio completo implica la aplicación de todos los dominios, lo cual significa un gran esfuerzo administrativo por parte de la empresa, por esta razón se referencian algunos de los dominios relacionados en la norma, uno de ellos lo constituye el dominio 5, denominado políticas de seguridad es el que se adaptara en la empresa con los controles 5.1.1 y 5.1.2 los cuales orientaran las directrices relacionadas con la seguridad de la información asignadas a una normatividad, legislación y controles de la empresa.

El propósito del objetivo de control del dominio 5 de la NTC ISO/IEC 27002:2013, es establecer directrices de la dirección en relación con la seguridad de la información y con base en ello contribuir a la alta dirección en la implementación de políticas de seguridad y el compromiso para su desarrollo adopción en la empresa.

Se busca a través de este instrumento conocer la percepción del área de sistemas en relación con el uso

de procedimientos, controles, normas y estándares de seguridad para mantener la integridad de la información en la empresa. Se aplica al jefe de sistemas.

5.2 Activos informáticos

Los activos informáticos corresponden a todos los elementos que componen el proceso de comunicación, es decir comprende la información, el emisor, el medio de transmisión y el receptor. En una forma detallada además de la información comprende los elementos hardware, software, la organización y las personas que la utilizan. Comprende los elementos esenciales para garantizar el funcionamiento adecuado del sistema informática.

Los activos informáticos hardware, comprenden la infraestructura., el cableado de red, los equipos de cómputo y los servidores, además los componentes relacionados con el software comprenden sistemas operativos, aplicaciones, programas de cómputo y por último la información que corresponde a bases de datos, paquetes de información, copias de información y claves.

Teniendo en cuenta los elementos que involucra se considera de vital importancia la evaluación de los activos informáticos ya que en general no corresponde simplemente a evaluar los recursos hardware y software desde el punto de vista de su utilización, sino en hacer un análisis general de todos los componentes que facilitan el acceso a la información y permiten mantener la integridad de la misma tanto a nivel físico, como lógico. Es decir comprende los recursos necesarios para garantizar el aseguramiento de la calidad de la información en CODELCAUCA.

5.3 Control de acceso [8]

El control de acceso tiene como objetivo permitir el acceso a la información, en este sentido relaciona acceso a las aplicaciones, privilegios, contraseñas y documentación.

Para garantizar el acceso a la información no solamente se requiere contar con una política que garantice un acceso seguro a la información, que facilita registro usuarios para acceder a los distintos servicios de red y de esta forma tener un control en con los registros de usuario.

Para garantizar un adecuado registro de usuario se debe partir de una adecuada gestión de usuarios, a partir del cual se genere una dinámica para el registro de usuarios, para la gestión de privilegios de usuario y claves de acceso, para la asignación de responsabilidades de usuario, de derechos de acceso, acceso a la red y políticas para garantizar un acceso responsable a los recursos del sistema de información.

En relación con la política control de acceso se aplicó un instrumento al jefe del área de sistemas de la empresa, con base en el cual se observa que tan robusto es la política relacionada con control de acceso.

5.4 Seguridad relacionada con el personal

La seguridad física debe ser referida como un sistema informático, y por lo tanto se debe generar la dinámica que permita salvaguardar la información relacionada con acceso no autorizado a cuarto de servidores o aplicaciones que deben ser solamente accedidas a personal autorizado [9].

En este sentido las funciones y obligaciones de cada una de las personas con acceso a datos de carácter personal y privado, así como a los sistemas de información estarán claramente definidas y documentadas de acuerdo a lo establecido en un documento físico. El responsable de un fichero deberá adoptar medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de las funciones así como las consecuencias que pudiera ocurrir en caso de incumplimiento.

Debe existir una correcta concienciación y formación de los usuarios que tengan acceso a los datos personales o privados, haciéndolos conocedores de la importancia y seriedad de la normativa y formándolos sobre funciones, obligaciones y normas que se debe cumplir.

5.5 Seguridad física y del entorno

Corresponde al dominio 9 de la norma, establece áreas seguras, y seguridad en equipos, y establece criterios para garantizar la seguridad y protección del sistema informático [10]. Para garantizar esta seguridad, se consideran di ferentes aspectos, como los que se describen a continuación:

- **Acceso físico a copias de seguridad**

El área de gestión tecnológica está conformada esta por cuatro personas el técnico programador, la persona de prestación de servicios, un pasante y una persona de contabilidad, lo que hace vulnerable al acceso físico a

las copias de seguridad u otros.

- **Almacenamiento de información**

La información de los usuarios críticos se guarda en unidades de red en una o varios dominios, haciendo vulnerable el acceso a la misma, pero estos accesos están limitados ya que existen carpetas compartidas en la red a la cual no se puede tener acceso, ya sea por privilegios, o no encuentre encendido un computador en especial.

- **Cuarto de servidores**

A los cuales solo tiene acceso el personal del área de gestión tecnológica, para realizar mantenimientos o instalaciones eléctricas, cableado, etc. El personal de mantenimiento de la empresa permanece, en algunas ocasiones, sin supervisión del área de gestión tecnológica en el cuarto de servidores.

- **Factores ambientales**

Se tiene accesorios de seguridad tales como un extintor de fuego esto se basa en la protección industrial, ya que las ventanas son de madera, las paredes son de cemento lo que da estabilidad a la estructura.

En el área de gestión tecnológica, cuarto de servidores y cuarto del rack de switches se tiene el peligro de un incendio y de cualquier inundación ya que las ventanas son de madera y a su vez se encuentran dañadas sin vidrio y quebradas es muy fácil de prender y la expansión de fuego es muy rápida y de que el agua de lluvia entre de cualquier forma.

6. Procedimientos considerados

Para definir una política de seguridad se tienen en cuenta procedimientos de registro de incidencias, respaldo de información, mantenimiento de equipos, restauración de copias de seguridad. Además la división de sistemas proporciona información en relación con la existencia de formatos que incluyen algunas tareas específicas del área de sistemas estos están relacionados con tareas como: mantenimiento correctivo de equipos de cómputo, administración de usuarios y cuentas de correo, inventario de equipos de cómputo, de servidores, hardware y software, de infraestructura de red, seguridad de la información y control de copias de seguridad.

7. Aplicación de Instrumentos

La base sustancial de esta propuesta es la aplicación de la política de seguridad de la información teniendo en cuenta lo planteado en los numerales 5.1.1 y 5.1.2 de la ISO/IEC 27002:2013, desde los cuales se dan directrices de seguridad de la información sujeta a normativas y controles propios que definirá la empresa, alrededor de la cual se establecen algunos puntos de referencia como son: la administración del sistema, privilegios de personal,

7.1 Gestión de activos

Gestión en sistemas de información es de suma importancia contar con tecnología que permita desarrollar diferentes actividades para el cumplimiento de los objetivos corporativos para lo se debe disponer de unos adecuados dispositivos de hardware y software que son el soporte del funcionamiento y procesamiento de la información.

7.2 Control de acceso

Los empleados deben utilizar adecuadamente la información o recursos y servicios informáticos haciendo un correcto uso de los mismos, accediendo de manera responsable a las cuentas de acceso que le permitan realizar de manera eficiente las actividades asignadas.

7.3 Seguridad física y del entorno

Este instrumento se aplica al administrador del sistema y busca su percepción en relación con el conocimiento del área de sistemas y el cumplimiento de lineamentos para cumplirla teniendo en cuenta la política de seguridad de la información. Se tiene en cuenta elementos como el almacenamiento de información, acceso del personal al área del servidor, la estructura física del área de sistemas, sistemas de alarma y protección, protección del ambiente informático.

7.4 Seguridad relacionada con el personal

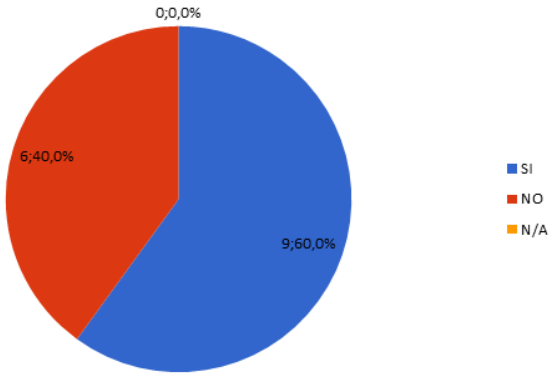
El talento humano juega un papel importante con el desarrollo de las actividades misionales de Codelcauca, en este compromiso no solo la alta dirección, sino todos los trabajadores de la empresa deben contribuir desde

sus puestos de trabajo y su compromiso con la empresa para mantener el un sistema de comunicación seguro y que por ende proporcione una buena calidad del servicio al usuario final.

8. Resultados

Se aplican instrumentos tanto al administrador de la red como al personal involucrado en el manejo de la información en relación a política de seguridad dominio 5 y la aplicación de los aspectos 5.1 y 5.2. Además se consideran otros dominios como activos informáticos, control de acceso, seguridad relacionada con el personal, seguridad física y ambiental, entre otros aspectos.

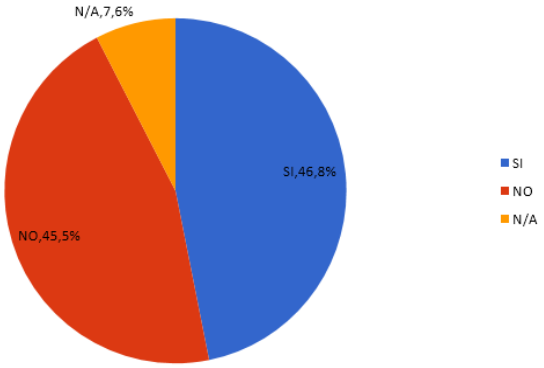
Las preguntas se realizaron de acuerdo a los dominios considerados para su estudio con sus respectivos controles, con base en ello se evalúa el nivel de conocimiento sobre seguridad de la información. A continuación a manera de ejemplo se han tomado unas preguntas.



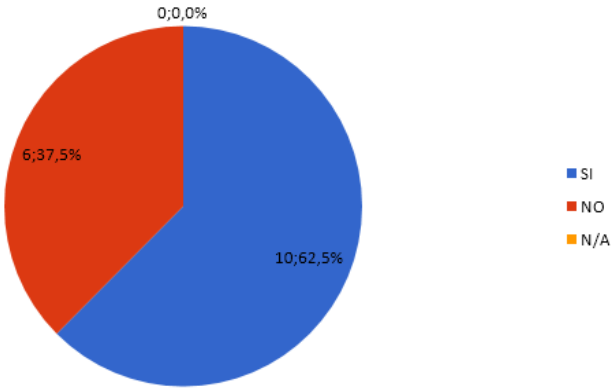
Gráfica 1. Evaluación de activos.

La evaluación de activos entrevista que se hizo al jefe de área de sistemas evidencia un conocimiento aceptable sobre los activos que posee la empresa donde se genera, se procesa y se crea información (gráfico 1).

En relación con el conocimiento relacionado con seguridad del personal se observa un nivel de conocimiento del 46.8%, frente a un 45.5 % de desconocimiento y un 7.6% no aplica, esta información se observa en la siguiente gráfica (gráfico 2).



Gráfica 2. Evaluación de seguridad relacionada con el personal.



Grafica 3 evaluación de política de seguridad

La evaluación de política de seguridad se realiza mediante entrevista aplicada al jefe de sistemas evidencia un conocimiento aceptable sobre política de seguridad de la información, tal como se indica en la siguiente gráfica (gráfico 3).

9. Conclusiones

La información es un activo esencial para Codelcauca, que debe ser protegida adecuadamente, pues actualmente el sector de los negocios está cada vez más interconectado y debido a esto la información está cada vez más expuesta a factores externos que afectan la integridad de la misma sea cual sea la forma en que se maneje los datos. La seguridad de la información se obtiene a través de la implementación de un conjunto adecuado de controles; donde se incluyan políticas,

procedimientos, estructuras organizacionales y funciones software y hardware.

Todas las áreas que manejan información sensible deben conocer sus responsabilidades en el manejo de la misma, para garantizar la debida protección de los datos con lineamientos que se adapten a las necesidades de la empresa.

Las directrices para adoptar una política de seguridad deben estar sujetas a una normatividad vigente que garantice su debida aplicación dentro de los lineamientos manejados por la empresa contando con un alto nivel de compromiso para llevar a buen término los objetivos de negocio propuestos para garantizar la protección de la información.

10. Referencias

[1] ISO 27000 Standars, «THE ISO 27000 DIRECTORY,» ISO 27000, [En línea]. Available:]http://www.27000.org/iso-27002.htm. [Último acceso: 20 I 2017].

[2] ISO, «ISO/IEC 27002:2013,» ISO/IEC 27002:2013, [En línea]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en. [Último acceso: 15 I 2017].

[3] T. Bradanovic, «Conceptos Básicos de Seguridad Informática,» [En línea]. Available: http://www.bradanovic.cl/pcasual/ayuda3.html. [Último acceso: 15 Dic 2016].

[4] ISO, [En línea]. Available: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/. [Último acceso: 12 2 2017].

[5] ISO, «CONTROLES DE ISO/IEC 27002,» [En línea]. Available: http://www.iso27000.es/download/ControlesISO27002-2005.pdf. [Último acceso: 12 03 2017].

[6] Coodelcauca, «Coodelcauca,» Coodelcauca, 2016. [En línea]. Available: http://codelcauca.com.co/. [Último acceso: 10 03 2017].

[7] Guatewireless, «Tareas y Responsabilidades del administrador del sistema,» [En línea]. Available: http://www.guatewireless.org/articulos/tareas-y-responsabilidades-del-administrador-del-sistema.html. [Último acceso: 25 03 2017].

[8] Panda, «Glosario,» [En línea]. Available: http://www.pandasecurity.com/spain/homeusers/security-info/glossary/. [Último acceso: 30 03 2017].

[9] ISO 27000, «ISO 27000,» [En línea]. Available: http://www.iso27000.es/sgsi.html. [Último acceso: 10 04 2017].

[10] «ISO 27002,» [En línea]. Available: https://iso27002.wiki.zoho.com/09SeguridadF%C3%ADsicayEntorno.html. [Último acceso: 20 04 2017].