IMPLEMENTACION DE SISTEMAS DE CONTROL DE LA INFORMACION EN EL SENA REGIONAL TOLIMA

TRABAJO DE GRADO

PARTICIPANTES

Códigos

ROMULO BETANCOURT
PABLO CESAR MONROY MARIN
JHONATAN CAMILO DAVILA

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2015

IMPLEMENTACION DE SISTEMAS DE CONTROL DE LA INFORMACION EN EL SENA REGIONAL TOLIMA

TRABAJO DE GRADO

PARTICIPANTES

Códigos

ROMULO BETANCOURT
PABLO CESAR MONROY MARIN
JHONATAN CAMILO DAVILA

Asesor(es)

Giovanny Andrés Piedrahita Solórzano

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

2015

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Ciudad, Fecha

INTRODUCCIÓN

Dentro de este documento se muestra la propuesta para un centro del SENA, directamente para los administrativos, directivos, contratistas instructores y aprendices, en la cual se hace un bosquejo que muestra la vulnerabilidad con la que cuenta la entidad y la falta de un sistema de información organizado, ya que en la actualidad no cumple con los lineamientos, política y estándares establecidos según la normatividad vigente.

En este orden de ideas se presenta alternativa de solución, y mediante un estudio no técnico que muestra el estado actual proponiendo una implementación de un sistema de información que cubra las necesidades y a su vez asesorados por especialista expertos en seguridad de la información con el objetivo de poner en marcha la normatividad propuestas, los lineamientos, estándares, y así contrarrestar algún tipo de riesgo y evitar la vulnerabilidad existente en materia de acceso a la información.

INDICE

AGRADECIMIENTO

Este proyecto es el resultado del esfuerzo conjunto de todos los que hemos conformado el grupo de trabajo desde un inicio hasta su finalización.
Por este medio agradecemos a nuestros jefes de la Regional Tolima por creer en nuestras capacidades para poner en práctica lo aprendido durante nuestros estudios como especialista de la seguridad de la información
El grupo conformado por Rómulo Betancourt Hortùa, Pablo Cesar Monroy y Jhonatan Camilo Dávila, quienes mediante el presente proyecto de investigación que duró varios meses nos sentimos satisfechos ya que ha llenado todas nuestras expectativas frente a la investigación realizada en nuestro ámbito de trabajo. A nuestros padres, familiares quienes han creído en nuestra prospectiva, a los tutores a quienes les debemos gran parte de sus conocimientos, gracias por la experiencia compartida y enseñanza. Para finalizar un gran agradecimiento a nuestra Universidad Politécnico Gran Colombiano.

1. Resumen Ejecutivo

1.1 Descripción general:

Dentro del Centro del SENA Regional Tolima, durante los últimos semestres se ha venido presentando incidentes en los datos de los directivos y administrativos, dichos incidentes se refieren a la pérdida de información, por tal motivo y con el fin de identificar el impacto causado y la frecuencia del suceso se elaboraron encuestas las cuales arrojaron como resultado que la entidad posee un alto riesgo que afecta la labor cotidiana; por ello existe la necesidad de implementar controles de seguridad para mitigar esta problemática.
Lo que se pretende es implementar diseños de salvaguardar la información en tiempo real para evitar un borrado accidental, sobre escritura de archivos, robo, incendio o siniestro (catástrofe naturales), daños en discos duros, virus, spyware entre varias amenazas que puede afectar al Centro; en este orden de ideas es importante contar con el apoyo de los directivos para implementar mecanismo y que los funcionarios apliquen estas normas para el buen uso de la información.

Es importante decir que se deben realizar copias de seguridad a diario, tener más de un soporte de copias, proteger el soporte de copia, identificar los activos más importantes, encriptar los archivos y para finalizar elaborar un plan de continuidad del negocio ante una posible situación que se presente.

Por tal motivo para el desarrollo de nuestro trabajo nos basamos como referencia en la norma TècnicaISO 27001 y la ISO 27002 ademas de esto nos documentamos y nos enfocamos en el alcance para dar a conocer los procesos o actividades que serán contempladas dentro del control.

Ahora bien cabe anotar las políticas de bajo nivel aplicadas para el funcionamiento del problema que actualmente se está evidenciando.

Este proyecto es importante ya que se propone dar como solución la realización de copias de seguridad para mitigar algún tipo de amenaza, riesgos, vulnerabilidad, ya que sin duda lo más relevante que tiene la entidad son los activos de información y por esto se plantea proponer políticas, lineamientos, y controles para salvaguardar la información.
A la fecha se presentan vulnerabilidades en los datos, ya que no se han establecido controles a los riesgos de pérdida de la información, es importante mencionar las situaciones presentadas entre otras los hurtos de portátiles con información la cual no posee ningún respaldo.

1.2 OBJETIVOS

1.2.1 Objetivo General

Proponer controles de seguridad de la información que permita diseñar estrategias para salvaguardar los datos en el centro del SENA Regional Tolima por medio de procesos, procedimientos, instructivos y guías para que sean desarrollados los requerimientos establecidos por la política general y así disminuir el riesgo ante las vulnerabilidades identificadas en el centro.

1.2.2 Objetivos Específicos

Identificar las vulnerabilidades y riesgos del centro regional Tolima SENA

Proponer medidas de seguridad de la información y que puedan ser aplicadas en las actividades laborales del SENA Regional Tolima.

Evaluar los mecanismos que permitirán una adecuada sensibilización al buen uso de la información.

Definir controles, lineamientos y políticas para minimizar los riesgos frente a los activos de información dentro de la organización.

Analizar algunas herramientas y modelos de seguridad de la información a las que se puede recurrir.

1.3 Alcance

Alcance:

Como primera medida este proyecto se compone de un documento con propuesta de normas que se deben aplicar para la protección de la información tomando como referencia las normas técnicas ISO 27001 y ISO 27002.

El alcance de este proyecto es seguir continuando con los términos del alcance mismo, ya que hay mucho procedimientos por realizar en el futuro, para un panorama de mejoras para el centro, y se seguirán proponiendo controles no solo de copias de seguridad si no de controles de acceso en las aulas físicas, realizando rutas de implementación con otras palabras este es el comienzo de la implementación de controles, políticas y lineamientos del centro de la Regional Tolima enfocados a proponer controles de seguridad de la información.

A continuación denominamos las variables tipo cualitativo y cuantitativo

TIPO	VARIABLES QUE INFLUYEN EN EL SISTEMA
Cuantitativas:	Aplicación de software en seguridad informática
	Controles, Lineamientos y políticas a establecer dentro de la organización
Cualitativas:	Capacitaciones en seguridad de la información y/o Brigadas del buen uso de la información

1.4 Entregables

A continuación presentamos los entregables:

Proyecto:
IMPLEMENTACION DE SISTEMAS DE CONTROL DE LA INFORMACION EN EL SENA REGIONAL TOLIMA.

Instructivos:
Paso a paso de cómo se deben de realizar los procesos para realizar copias de seguridad.

Herramientas:
Aplicación de herramientas criptográficas de confidencialidad y autenticidad.

Capacitaciones:
Sensibilizar a los Directivos y Funcionarios con el fin de mitigar la pérdida de información.

Descripción
En vista de todo lo argumentado y los estudios establecidos, el centro apoya al equipo ejecutor de la seguridad de la información, los directivos invierten en ello y obligan al área administrativa e instructores a evitar riesgos, vulnerabilidades para que en el futuro no se esté lamentando la pérdida innumerable de datos. Los directivos son conscientes que puede existir un tercero que pretenda acceder a la información y que con estos lineamientos será baja la fuga de información por mala manipulación en el espacio laboral y o personal.

1.5 Cronograma
Diferenciar el cronograma del proyecto de grado del cronograma del proyecto completo.

PLAN DE TRABAJO

FASE	ACTIVIDAD	TIEMPO
PLANEACION	Encuestas a los contratistas, directivos y administrativos	1 MES
	Levantamiento de datos	
	Definir las directrices a seguir para implementación de la seguridad.	
	Prueba piloto para la alternativas de la solución propuesta	
	Sustentación del proyecto a presentar	
DISEÑO	Implementación de políticas de seguridad de información	2 MES
	Diseño de la implementación de controles de acceso a los sistemas	
	Diseño y análisis de la implementación de políticas	
	Actividades en el proyect para la realización y construcción del proyecto de seguridad	
IMPLEMENTACION	Apropiación y configuración de herramientas	3 MES

	• Clasificación de los datos • Implementación de nuevos controles de seguridad de la información	
	Implementación de formatos para manejar los registros relacionados con la seguridad de la información	
	Implantación y mejoramiento para tener respaldos de la información	
	Ejecución de la sensibilización sobre la importancia de seguridad de la información	
	Implementación de los controles y políticas ya establecidas a carga de los gestores especializados.	
SEGUIMIENTO	Análisis de control acceso y perdida de información	4 MES
	Reflexiones de las medidas tomadas mediante los indicadores requerido	

2. JUSTIFICACIÓN

Dentro del centro del SENA de Regional Tolima se han venido presentando problemas de perdida de datos que conllevo a que se realizara una investigación con el fin de determinar las posibles causas obteniendo como resultado que durante el año 2014 aumento en un 40% la cantidad de datos perdidos de la misma manera para el año 2015, por esta razón se determinó que los activos de información han sido vulnerados y existe alto riesgo para el centro en materia legal y reputacional; se ha incrementado este problema ya que los indicadores de las encuestas realizadas los dos últimos años aumentaron lo cual preocupa a la entidad. Con esto se busca disminuir estos indicadores y garantizar una protección segura de los datos para mitigar la perdida de información para los funcionarios.

El presente proyecto plantea como propuesta lineamientos para salvaguardar los datos que pretenden sustentar la importancia de tener seguro los activos de información y posteriormente se representara por medio de un gráfico los datos reales de las entrevistas que se realizaron a los 60 funcionarios de la entidad del año anterior y el actual (encuestas 2014 y encuestas 2015).

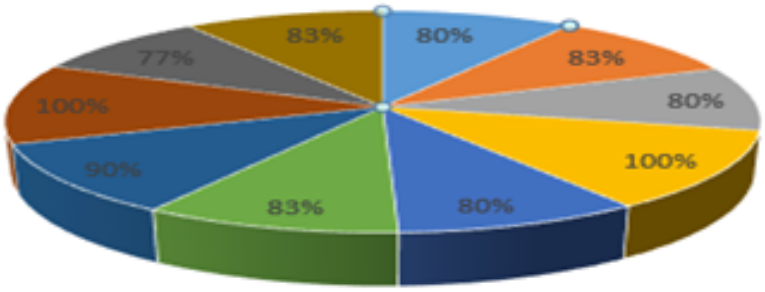
La meta para el 2016 es contar con controles establecidos y que para las próximas encuestas no encontremos riesgos asociados a la misma, sino por el contrario se vea beneficiada la entidad por el buen uso de la información, a manera de indicadores, contar con un 90% del impacto positivo y reducir al máximo los incidentes de riesgos.
Es importante que se haga realidad este proyecto y más como opción de grado para dejar huella en la entidad como es el centro de la Regional Tolima, ya que si no se realizan los controles en el centro los riesgos y amenazas pueden aumentar y en un periodo determinado tener pérdidas económicas, reputacionales y legales en la institución, aparte de esto al ser auditados por dirección general y podemos correr el riesgo de no tener la información cuando se necesite.

A partir de las fase de un P.H.V.A se formularon soluciones para tener el control de cómo es que se va a proponer esta política en la institución. Nos obstante se requiere primero que todo, concientizar a los funcionarios para minimizar la perdida de información. Para su mayor entendimiento se entregara un paso a paso de cómo se aplicara la respectiva solución y una duración de un tiempo de 4 meses ya que no se puede dejar pasar más tiempo, en la cual se debe realizar la planeación, diseño, implementación y seguimiento así como esta descrito en el plan de trabajo y para finalizar el entregable que es el producto para la institución y poner en marcha su funcionalidad.

Se tendrá un impacto positivo para el centro dentro de la Regional Tolima cuyo objetivo es contar con los controles de seguridad de la información y ser pioneros dentro de los centros del Tolima, ya que los demás no cuentan con ello.
Dentro de la institución se crearon políticas de seguridad en cuanto al cuidado físico y no se obtuvo un gran impacto ya que los directivos no vieron importante hacer cumplir este control por el hecho de la inversión como tal. Partiendo del

riesgo que ocurrió en la falla de equipos los directivos ven la necesidad de crear políticas de seguridad como tal para la entidad, por esto empezaremos por el activo más importante que es la copia de seguridad de los datos en tiempo real.

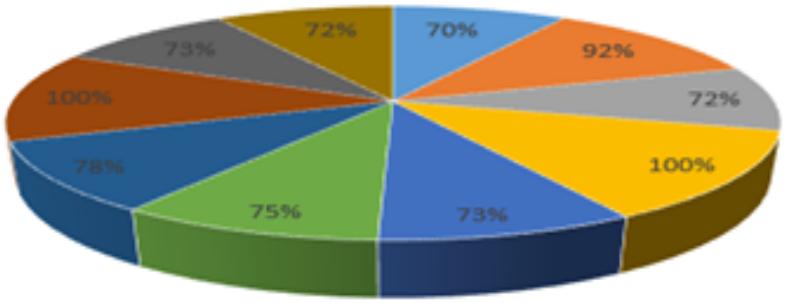
2015 ENCUESTAS



80%
83%
80%
100%
80%
83%
90%
100%
77%
83%

1) Usted realiza backup de la información
NO
2) Si respondió si entonces donde almacena la información
Memorias flash o discos duros de la empresa
3) Alguna vez ha perdido información
SI
4) Cada cuanto se realizan jornadas de sensibilización con respecto a la seguridad de la información
Nunca
5) Sus contraseñas en el aplicativo, son compartidas
SI
6) Lleva información de la entidad a su casa en una USB, disco duro, u otro dispositivo de almacenamiento
SI
7) Si respondió si ¿Por qué lleva información de la oficina a la casa?
Para adelantar trabajo
8) Cuáles de las siguientes páginas de internet usted accede normalmente
Todas las anteriores
9) Usted conecta a su computador dispositivos de almacenamiento masivo
Memorias USB
10) Cuando está en la organización trabaja con su computador personal o con el que le asigno en centro:
Computador del centro

2014 ENCUESTAS



70%

1) Usted realiza backup de la información

NO

92%

2) Si respondió si entonces donde almacena la información

Memorias flash o discos duros de la empresa

72%

3) Alguna vez ha perdido información

SI

100%

4) Cada cuanto se realizan jornadas de sensibilización con respecto a la seguridad de la información:

Nunca

73%

5) Sus contraseñas en el aplicativo, son compartidas

SI

75%

6) Lleva información de la entidad a su casa en una USB, disco duro, u otro dispositivo de almacenamiento:

SI

78%

7) Si respondió si ¿Por qué lleva información de la oficina a la casa?

Para adelantar trabajo

100%

8) Cuáles de las siguientes páginas de internet usted accede normalmente

Todas las anteriores

73%

9) Usted conecta a su computador dispositivos de almacenamiento masivo

Memorias USB

72%

10) Cuando está en la organización trabaja con su computador personal o con el que le asigno en centro:

Computador del centro

Indicadores:
[1] Tomado de la información en empresas colombianas

Resultados	Fuentes de información	Medición	Nombre del indicador
81 % de las empresas nunca ha implementado una herramienta	Cifras Suministradas por Directivos y Administrativos.	Volumen de Registros en la Pérdida de Datos en los portátiles personales, en el	Vulnerabilidad de los Datos En empresas y Entidades en Colombia.

para gestión de riesgos. 53% ha instalado antivirus en todas las tecnologías de su empresa incluyendo las móviles. 40% NO revisa el marco normativo de seguridad de la información implementando en la empresa 52% no ha implementado en su empresa ningún estándar internacional de Infosec 47% nunca hizo ningún test de seguridad de las redes (Ethical Hacking, Análisis De Vulnerabilidades y/o Pruebas De Penetración en su empresa) 47% no cuenta con un Plan de Continuidad del Negocio que le permita seguir con las operaciones en caso de un evento no deseado.	Careto Año: 2014. • Objetivo: Campaña de Ciberespionaje iniciada desde 2007, que robaba información a agencias gubernamentales. KPMG: El 13% de los ilícitos que se han cometido en el último año contra de empresas que operan en Colombia y generando un daño económico cercano a los 550 millones de dólares. El 23 % de los ataques cibernéticos pueden atribuirse a la deslealtad de empleados, el 20% se debe a fallas en la seguridad de la tecnología utilizada en las compañías afectadas y un 17% al robo de dispositivo móvil.	periodo Semestral (Directivos y Administrativos) Cantidad de Archivos Infectados por Mal uso de Antivirus en los equipos asignados a los Directivos, Administradores y Aprendices Pérdida de la información de muchos años de información a causa de un posible hurto	Ciberespionaje

	el 27% tuvo daños económicos, el 21% sufrió la pérdida de información sensible y el 15% fue objeto de extorsión y chantaje El 39% de los cibercrimenes se detectaron accidentalmente, es decir, fueron identificados fortuitamente o al azar. El 30% fue bloqueado por los mecanismos de control interno y el 17% por alguna denuncia. el 53% de los cibercrimenes se detectaron después de un mes de haberse realizado el ataque		
0/4 Meta: 4/4	Encuestas de los Directivos y Administrativos de la Vulnerabilidad de la información	Brigadas del buen uso de realizar Backup de Datos, Realizar copias día a da	Campañas de Seguridad de la Información

2.1 ¿Qué necesidades está satisfaciendo?

Las necesidades que se están satisfaciendo es mitigar la pérdida de información, porque este es el activo más importante para el centro, en este orden de ideas es minimizar las vulnerabilidades de los riesgos que se puedan presentar.

2.2 ¿Qué beneficios se logran al solucionar la necesidad?

Los beneficios que se logran al solucionar la necesidad es la implementación de controles, lineamientos y políticas de seguridad de la información con el fin de salvaguardar los activos.

En la mayoría de la organizaciones a nivel mundial la seguridad de la información es muy indispensable por la gran cantidad de información que se manejan pero a la vez se generan muchos riesgos para el manejo de esta misma por otro lado los ataques cibernéticos cada día vienen en aumentando, Colombia es el sexto país en ocupar el lugar de Ciberdelincuentes e incumplen la ley 1273 de la protección de la información y de los datos; partiendo de ello es importante saber que el mundo de la informática, esta propensa a una actividad criminal, causante del 13% de los ilícitos que se han cometido en el último año contra de empresas que operan en Colombia y generando un daño económico cercano a los 550 millones de dólares. El 23% de los ataques cibernéticos pueden atribuirse a la deslealtad de empleados, el 20% se debe a fallas en la seguridad de la tecnología utilizada en las compañías afectadas y un 17% al robo de dispositivo móvil.
Dentro de las encuestas realizadas por KMPG en el año 2013 se investigó que el 27% tuvo daños económicos, el 21% sufrió la pérdida de información sensible y el 15% fue objeto de extorsión y chantaje. El 39% de los cibercriminales se detectaron accidentalmente, es decir, fueron identificados fortuitamente o al azar. El 30% fue bloqueado por los mecanismos de control interno y el 17% por alguna denuncia. [**2]**

Por último es muy importante vivir informado y saber las amenazas y vulnerabilidades que se presentan en el medio y tener planes de contingencia para dichos eventos para poder reducir los ataques a la información de las organizaciones, En este orden de ideas es importante aclarar que la Regional Tolima SENA, requiere centrarse en buscar soluciones para contrarrestar una posible vulnerabilidad en los datos.

El gasto en seguridad de la información habrá crecido 4,7 por ciento a nivel global para fines de 2015, alcanzando los 75.400.000.000 dólares en total.
Esto se desprende de un nuevo análisis de Gartner, que afirma que el aumento en la inversión se puede atribuir a varios factores, incluyendo mayor legislación, más iniciativas de gobierno y los aprendizajes tras brechas de datos de alto impacto.
Todo esto remarca la severidad del cibercrimen en la actualidad, ya sea desde el punto de vista de un individuo, organización o gobierno. “El interés en las tecnologías de seguridad es impulsado cada vez más por elementos de negocio digitales, en particular la nube, la computación móvil y ahora también la Internet de las Cosas, así como por el carácter sofisticado y de alto impacto de los ataques dirigidos avanzados **[3]**

3. MARCO TEÓRICO Y REFERENTES

Dentro de la Entidad de la Regional Tolima se da la necesidad de proponer controles de seguridad de la información para mitigar los riesgos, amenazas y vulnerabilidades teniendo en cuenta que se debe de proteger la triada CID, con ello

se buscaron soluciones previas para evitar pérdidas de información, la cual estamos enfrentando el problema de que en el Centro del SENA Tolima durante los últimos semestres se han venido presentando vulnerabilidades en los datos de los directivos y administrativos. Nos apoyamos como guía de la familia ISO y de metodologías en cuanto a la seguridad de la información.

4. METODOLOGÍA

La metodología que se propone diseñar está basada en la norma ISO 27001 y ISO 27002, con la cual se busca cumplir todos los objetivos generales y específicos para llegar a su máximo logrado.

Las fases que se implementaron fueron:

Primera fase

Es esta fase implementamos una aplicación de encuestas para los administrativos y funcionarios con un total de 11 preguntas que están relacionadas con la seguridad de la información basado en realizar copias de seguridad la cual fueron encuetados 60 funcionarios del centro.
Esto se realizó con el fin de verificar como están salvaguardando los datos, y como objetivo concientizarlos del buen uso de ellas.

Encuestas: Esto se realizó con el fin de hacer un muestreo de como los empleado están manejando la información y con el objetivo de hacer realidad los lineamientos del año 2014 y 2015

Segunda fase

Dentro de esta fase se realizó un análisis de encuestas para determinar cuáles son las preguntas con mayor riesgo y que puede ser una amenaza para entidad de igual manera mitigar la vulnerabilidad, se desarrolló una estadística de cada pregunta y se obtuvo gráficos, permitiendo identificarlos el nivel más alto de riesgo, este análisis es completo. Se describen los actores relevantes.

Tercera fase

Después de haber realizado las encuestas y su análisis de cada una de ellas, se propone crear controles, diseños y políticas para salvaguardar la información por medio de copias de seguridad en tiempo real.
Esta actividad se desarrolló con el fin de saber cuál es la amenaza frente al mal uso de los datos, por esto se entrega un documento de los controles que se deben de tener en cuenta a la hora de su implementación, con el fin de mitigar las vulnerabilidades
Como idea principal es que lo lineamientos que se creen se cumplan para Minimizar los riesgos de la perdida de la información.

4.1 Encuestas:

La encuesta se aplicó a los empleados administrativos y Directivos.
Cantidad Entrevistado: 60 Personas
Encuesta: Aleatoria

¿Usted realiza Backup de la información?	RESULTADOS	PORCENTAJE
SI	12	20%
NO	48	80%
TOTAL	60	100%
Si respondió si entonces donde almacena la información	RESULTADOS	PORCENTAJE
Memorias flash o discos duros de la empresa	9	75%
Memorias flash o discos duro personal	2	15%
Google drive	1	10%
TOTAL	12	100%
¿Alguna vez ha perdido información?	RESULTADOS	PORCENTAJE
SI	48	80,00%
NO	12	20,00%
TOTAL	60	100,00%
¿Cada cuanto se realizan jornadas de sensibilización con respecto a la seguridad de la información?	RESULTADOS	PORCENTAJE
Trimestralmente	0	0,00%
Semestralmente	0	0,00%
Anualmente	0	0,00%
Nunca	60	100,00%
TOTAL	60	100,00%
¿Sus contraseñas en el aplicativo, son compartidas?	RESULTADOS	PORCENTAJE
SI	48	80,00%
NO	12	20,00%
TOTAL	60	100,00%
¿Lleva información de la entidad a su casa en una USB, disco duro, u otro dispositivo de almacenamiento?	RESULTADOS	PORCENTAJE
SI	50	83,33%
NO	10	16,67%
TOTAL	60	100,00%
Si respondió si ¿Por qué lleva información de la oficina a la casa?	RESULTADOS	PORCENTAJE

Para llevar copia de seguridad a la casa	6	10,00%
Para adelantar trabajo	54	90,00%
TOTAL	60	100,00%
¿Cuáles de las siguientes páginas de internet usted accede normalmente?	RESULTADOS	PORCENTAJE
a) Redes sociales	0	0,00%
b) Mensajería	0	0,00%
c) Información	0	0,00%
d) Plataformas	0	0,00%
e) Música	0	0,00%
F) Todas las anteriores	60	100,00%
TOTAL	100	100,00%
¿Usted conecta a su computador dispositivos de almacenamiento masivo?	RESULTADOS	PORCENTAJE
a. Memorias USB	46	76,67%
b. Disco duro externo	3	5,00%
c. Teléfono celular	11	18,33%
d. Ninguna	0	0,00%
TOTAL	60	100,00%
Cuando está en la organización trabaja con su computador personal o con el que le asigno en centro:	RESULTADOS	PORCENTAJE
a) computador personal	10	16,67%
b) computador del centro	50	83,33%
TOTAL	60	100,00%
En alguna ocasión cuando le hayan realizado cambio de computador perdió información	RESULTADOS	PORCENTAJE
a) Si	38	63,33%
b) No	22	36,67%
TOTAL	60	100,00%

Con la anterior tabla se muestra la importancia que se debe proponer controles de seguridad de la información en este caso de aplicar proceso y actividades de realizar copias de seguridad dentro del centro del SENA la regional Tolima

4.2 ANALISIS DE ENCUESTA

La encuesta que se realizó en el centro Regional Tolima se elaboró con el fin de evaluar el estado de la entidad, en el que actualmente se está evidenciando la

problemática, se hizo con el propósito de identificar la situación y ver la necesidad de la seguridad de la información que es muy importante a la hora de aplicar.
Esta encuesta se realizó a 60 funcionarios del centro con una cantidad de 11 preguntas, con ello podremos identificar cual es el riesgo más vulnerable que a continuación describiremos uno a uno

El resultado de las encuestas que realizamos nos indican que:

Los administrativos, no cuentan o no reportan adecuadamente los incidentes relacionados con la perdida de la información.

No se realiza ningún control por parte de los funcionarios ya sean directivos y administrativos sobre la copia de información.

Los administradores son muy flexibles con las claves personales de la plataforma.

Una vez identificadas las vulnerabilidades se encontró que el equipo administrativo posee el más alto nivel de riesgo.

4.3 DOCUMENTOS DE LA PROPUESTA

Procesos, procedimientos y guías para llevar a cabo los controles en la organización que permitirán salvaguardar la información y mitigar las amenazas de perdida de los datos.

5. RESULTADOS Y DISCUSIÓN

Dentro los resultados alcanzados se realizó un estudio preliminar entre los cuales nos basamos en los objetivos de la propuesta de un SGSI que permite diseñar políticas; la idea principal es promover medidas de seguridad de la información y que puedan ser aplicadas en las actividades laborales, no obstante identificando las vulnerabilidades y riesgos de la entidad teniendo en cuenta que se realizarán campañas de sensibilización.

Los controles que se proponen para este proyecto de seguridad de la información entre los que se destacan para cumplir con la necesidad son:

Implementación de antivirus licenciado

Sistema criptográfico: Proponer utilizar software de encriptación para él envió de archivos vía e-mail.

Seguridad y afines: Identificar la infraestructura física de la entidad con el fin de establecer factores de riesgos.

Controles, políticas y lineamientos de la entidad: Capacitación de sensibilización de la seguridad de la información.

Campañas de culturización y de sensibilización para salvaguardar los activos.

Las dificultades que nos presentaron fue la aplicación de la encuesta porque son muy desconfiados a la hora de suministrar información, teniendo en cuenta que se les advertía que se hace para un fin de aseguramiento.

Es importante decir que este proyecto se hace realidad con el apoyo de los Directivos que se registre dentro de las políticas establecidas de la entidad.

Es por ello que se levantaran todos los documentos más relevantes y que implementen las fases del proceso de aseguramiento y prevenir la perdida de información realizando copias de seguridad (backup).

En relación a los objetivos específicos, no se están cumpliendo a cabalidad:

Dentro de la organización no se están realizando los mecanismos necesarios que permitan cumplir con los objetivos específicos para salvaguardar la información como son:

- Controles de acceso en áreas físicas mediante sistema biométrico
- Protección contra intrusos en la redes de datos
- Bloqueo a través del acceso web a usuarios no autorizados
- Identificación de vida útil del parque tecnológicog

6. CONCLUSIONES

Se concluye que partiendo de una necesidad del centro regional Tolima del SENA se ve la prioridad de proponer controles y lineamientos para salvaguardar la información administrativa que por muchos años la tienen en sus computadoras sin ninguna copia de seguridad. La entidad no cuenta con lineamientos frente al tema de implementar controles de seguridad de la información en este caso de realizar copias de seguridad.

Este proyecto nos permitió identificar y aplicar conceptos de seguridad de la información que se encuentran en las diferentes normas y metodologías existentes así como la aplicación y puesta en práctica en una entidad del sector público.

7. BIBLIOGRAFÍA

[1] Inseguridad de la información de la empresa Colombiana. Tomado de http://www.infosecurityvip.com/newsletter/estadisticas_ago11.html. Consulta del año anterior, 2014

[2] Encuesta de Fraude en Colombia en 2013 KPMG. Tomado de https://www.kpmg.com/CO/es/IssuesAndInsights/ArticlesPublications/Documents/Encuesta%20de%20Fraude%20en%20Colombia%202013.pdf Consulta realizada en 2013.

[3] El gasto de seguridad de la información crece 4,7% en 2015 a nivel global. Tomado de http://www.welivesecurity.com/la-es/2015/09/24/gasto-en-seguridad-de-la-informacion-crece/ Consulta realizada 24 de septiembre del 2015.

http://www.trendmicro.es/informacion-seguridad/investigacion/trendlabs-2013-annual-security-roundup/index.html

http://www.raing.es/es/sites/default/files/20140514_INT_RAIng_INTECO_EGD_V0.pdf%20INTECO

http://www.gerente.com/detarticulo.php?CodArticl=935

8. ANEXOS

LISTA DE ANEXOS:

1. Encuestas administrativos y funcionarios de la entidad.

2. Análisis de las encuestas.

3. Entregable para proponer los controles, diseños para la seguridad de la información.